



FASHION
LAW
BOOT
CAMP®

SPECIAL EDITION

FASHION & TECHNOLOGY

JULY 26-28, 2017
SAN FRANCISCO / CUPERTINO



FASHION LAW
INSTITUTE®



FASHION LAW INSTITUTE®

Fashion Law Bootcamp: Special Edition 2017
Fashion & Technology
San Francisco/Cupertino
July 26-28, 2017

Welcome – and for some of you, welcome back – to Fashion Law Bootcamp! Since launching the original Fashion Law Bootcamp summer intensive program, we've periodically offered in-depth, specialized programs on specific subjects at your request. And where better to take up the timely topic of fashion & technology than in Silicon Valley? Thanks to our original West Coast partner, Levi Strauss & Co., for their vision and ongoing hospitality, to The RealReal (and our Bootcamp alumnus, Sr. Director of Authentication & Brand Compliance Graham Wetzberger) for inviting us to visit for the first time, to Apple for once again giving us unmatched access to their campus, and to all of you for joining us!

Fashion & technology have a long history together, and technological innovation has always moved fashion forward. From needle to spindle, loom, sewing machine, digital printing, and now the advent of 3D printing, new production technologies have been key to the evolution of fashion. The Jacquard loom was a particularly pivotal point, since it was also the precursor of the modern computer.

For most of human history, however, even as production techniques became more sophisticated, the primary function of clothing was the same: to cover the body and to protect it. Today, we are reimagining the function of clothing itself and designing a myriad of new possibilities, both aesthetic and utilitarian. Fashion in the past has served to represent each of us to the world; now it can connect us to the world.

In addition, information technology in particular is currently reshaping distribution, sales, advertising, and the culture of the fashion industry itself – and, predictably, raising legal issues. This intensive program is organized around the effects of successive technological advances on the areas of fashion production, distribution, and ultimately the products themselves. Topics include intellectual property, licensing, and anticounterfeiting; venture capital and other financing structures; advertising, social media, and social commerce; supply chain monitoring and management; safety; and privacy.

Onward to the legal and business developments that are shaping the future of fashion!

Summary itinerary: Wednesday, July 26
Levi Strauss & Co. global headquarters
Levi's Plaza, 1160 Battery Street, San Francisco, CA
3:15-3:30pm – check-in the lobby outside the Archive
3:30-4:30pm – program
4:30-5:30pm – welcoming reception at Il Fornaio

Thursday, July 27

The RealReal central operations center – **bring photo ID**
3745 Bayshore Blvd., Brisbane, CA

8:45am sharp – take “San Francisco Mini Bus” shuttle from Glen Park BART station to The RealReal and exit at drop off point C. This is The RealReal’s regular employee shuttle and will not wait, so please allow extra time to arrive at the Glen Park BART station and board the shuttle by 8:40am.

9:15am-5pm – program

5:15pm – leave The RealReal on return shuttle to Glen Park BART station

Friday, July 28

Apple’s global headquarters, Cupertino, CA – **bring photo ID**

7:45-8am – meet on the south side of Union Square, Geary Street between Powell & Stockton (mini-bus departs at **8am sharp**. If you are traveling separately, email bootcamp@fashionlawinstitute.com for directions & parking information.)

10:30am-6pm – program

6pm – leave Apple and return to San Francisco

Contacts: Associate Director Jeff Trexler, jeff@fashionlawinstitute.com
Professor Susan Scafidi, Founder & Director, scafidi@law.fordham.edu
Assistant Director Pamela Golkin-Moro, pam@fashionlawinstitute.com

Requirements: All Bootcamp participants are expected to fulfill the following requirements:
(1) attend speakers’ sessions. In particular, attorneys seeking continuing legal education credit must be sure to sign the attendance sheet each day. CLE rules indicate that attorneys who miss all or a substantial part of any session cannot receive credit for that session.
(2) engage in classroom discussion and, time permitting, ask questions of speakers. There is no greater compliment to a speaker than to ask a question and no better way to learn than to formulate thoughtful inquiries. (Reading materials are provided for subsequent reference – in thematic wearable tech form for ease of transportation – and we hope that you’ll continue to inquire, think, and learn!)

Credits: 12 California MCLE (60-minute hours),
14 New York CLE (50-minute hours)



FASHION LAW INSTITUTE

FASHION LAW BOOTCAMP: SPECIAL EDITION FASHION & TECHNOLOGY

Wednesday, July 26, 2017

From Fig Leaves Forward: Fashion & Technological Advances in Historical Context

Readings

U.S. Patent No. 139,121, Improvement in Fastening Pocket Openings, May 20, 1873.

Complaint, In the Matter of Certain Laser Abraded Denim Garments, International Trade Commission, August 18, 2014.

U.S. International Trade Commission, News Release: USITC Institutes Section 337 Investigation of Certain Laser Abraded Denim Garments, September 17, 2014, https://www.usitc.gov/press_room/news_release/2014/er0917mm1.htm.

Levi's Settles ITC Patent Infringement Case, Rivet, February 9, 2015, <http://rivetandjeans.com/levis-settles-itc-patent-infringement-case/>.

U.S. Patent Application No. 14/959,730, Publication No. 20160282988, Two Layer Interactive Textiles (published September 29, 2016).

John Brownlee, *Inside the Design of Google's First Smart Jacket*, Fast Company, May 23, 2016, fastcodesign.com/3060133/inside-the-design-of-googles-first-smart-jacket.

Rachel Metz, *Here's Why Google and Levi's Are Working Together to Make a Jean Jacket*, MIT Technology Review, May 26, 2016, <https://www.technologyreview.com/s/601564/heres-why-google-and-levis-are-working-together-to-make-a-jean-jacket>.

Katie Berrington, *Vogue Meets Levi's Historian*, Tracey Panek, Vogue UK, July 25, 2016, vogue.co.uk/news/2016/07/25/tracey-panek-levis-historian-interview.

U.S. Patent No. 9,624,608 B2, Architecturally Reinforced Denim, April 18, 2017.

Kali Hays, *Nike's New Patent Could Mark the Rise of Ath-Denim*, WWD, April 21, 2017, <http://wwd.com/business-news/technology/new-nike-patent-could-mark-the-rise-of-ath-denim-10872474/>.

Sharon Edelson, *Nike Just Does It: Applies Footwear to Apparel*, WWD, July 12, 2017, <http://wwd.com/fashion-news/activewear/nike-just-does-it-applies-footwear-technology-to-apparel-10943412/>.

Vibrating Connected Jeans, Spinali Design, <https://www.spinali-design.com/pages/vibrating-connected-jeans>.

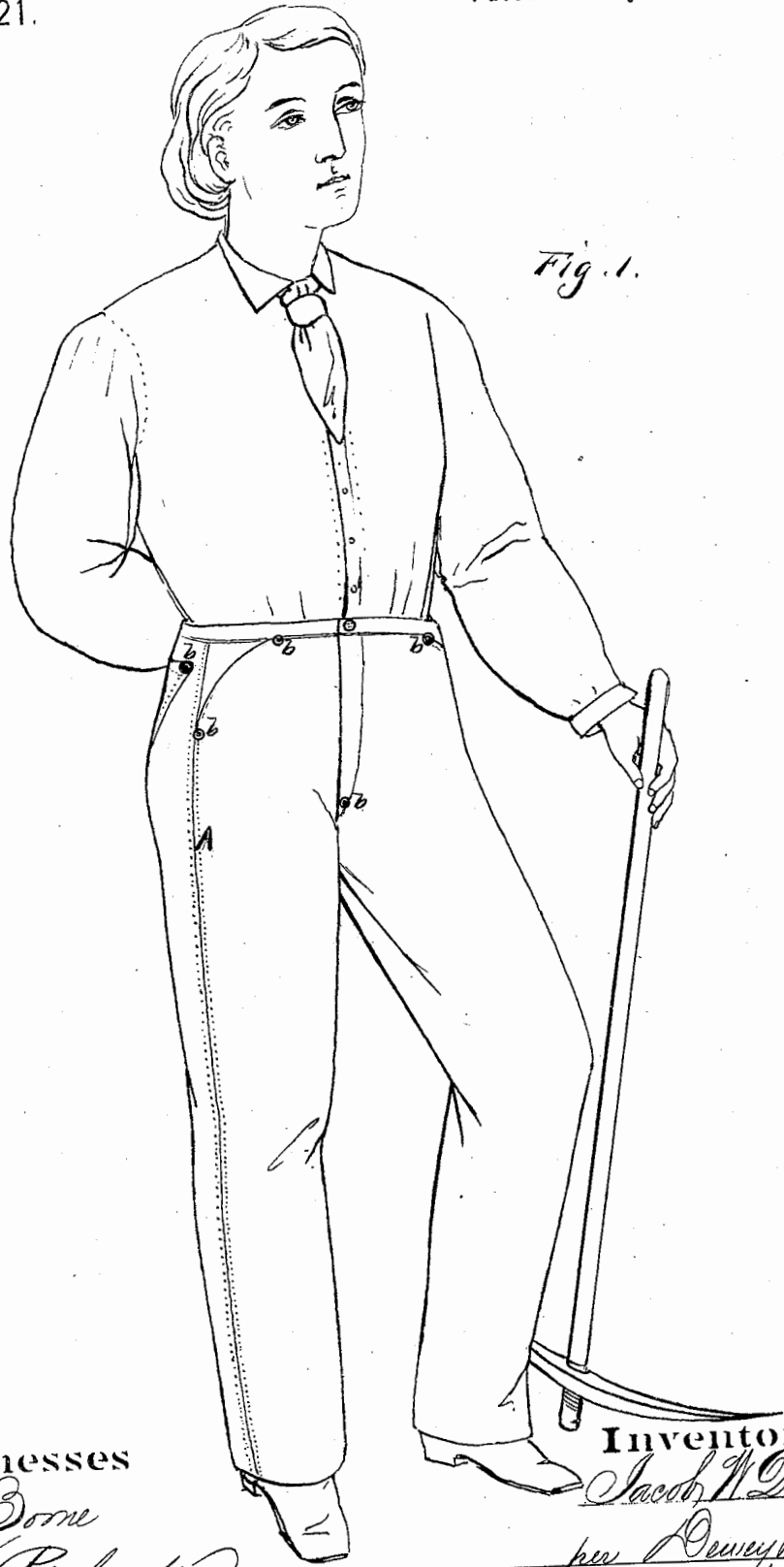
About, Spinali Design, <https://www.spinali-design.com/pages/vibrating-connected-jeans>.
<https://www.spinali-design.com/pages/about-us>.

Susan Scafidi, *FIT: Fashion as Information Technology*, 59 Syracuse L. Rev. 69 (2008).

J. W. DAVIS.
Fastening Pocket-Openings.

No. 139,121.

Patented May 20, 1873.



Witnesses

J. L. Bone
C. M. Richardson

Inventor

Jacob W. Davis
 per *Dwight G. Atlys*

UNITED STATES PATENT OFFICE.

JACOB W. DAVIS, OF RENO, NEVADA, ASSIGNOR TO HIMSELF AND LEVI STRAUSS & COMPANY, OF SAN FRANCISCO, CALIFORNIA.

IMPROVEMENT IN FASTENING POCKET-OPENINGS.

Specification forming part of Letters Patent No. **139,121**, dated May 20, 1873; application filed August 9, 1872.

To all whom it may concern :

Be it known that I, JACOB W. DAVIS, of Reno, county of Washoe and State of Nevada, have invented an Improvement in Fastening Seams; and I do hereby declare the following description and accompanying drawing are sufficient to enable any person skilled in the art or science to which it most nearly appertains to make and use my said invention or improvement without further invention or experiment.

My invention relates to a fastening for pocket-openings, whereby the sewed seams are prevented from ripping or starting from frequent pressure or strain thereon; and it consists in the employment of a metal rivet or eyelet at each edge of the pocket-opening, to prevent the ripping of the seam at those points. The rivet or eyelet is so fastened in the seam as to bind the two parts of cloth which the seam unites together, so that it shall prevent the strain or pressure from coming upon the thread with which the seam is sewed.

In order to more fully illustrate and explain my invention, reference is had to the accompanying drawing, in which my invention is represented as applied to the pockets of a pair of pants.

Figure 1 is a view of my invention as applied to pants.

A is the side seam in a pair of pants, drawers, or other article of wearing apparel, which terminates at the pockets; and *b b* represent the rivets at each edge of the pocket opening. The seams are usually ripped or started by the placing of the hands in the pockets and

the consequent pressure or strain upon them. To strengthen this part I employ a rivet, eyelet, or other equivalent metal stud, *b*, which I pass through a hole at the end of the seam, so as to bind the two parts of cloth together, and then head it down upon both sides so as to firmly unite the two parts. When rivets which already have one head are used, it is only necessary to head the opposite end, and a washer can be interposed, if desired, in the usual way. By this means I avoid a large amount of trouble in mending portions of seams which are subjected to constant strain.

I am aware that rivets have been used for securing seams in shoes, as shown in the patents to Geo. Houghton, No. 64,015, April 23, 1867, and to L. K. Washburn, No. 123,313, January 30, 1872; and hence I do not claim, broadly, fastening of seams by means of rivets.

Having thus described my invention, what I claim as new, and desire to secure by Letters Patent, is—

As a new article of manufacture, a pair of pantaloons having the pocket-openings secured at each edge by means of rivets, substantially in the manner described and shown, whereby the seams at the points named are prevented from ripping, as set forth.

In witness whereof I hereunto set my hand and seal.

JACOB W. DAVIS. [L. S.]

Witnesses:

JAMES C. HAGERMAN,
W. BERGMAN.

**UNITED STATES INTERNATIONAL TRADE COMMISSION
WASHINGTON, DC**

In the Matter of
CERTAIN LASER ABRADED DENIM
GARMENTS

Investigation No. 337-TA-___

**VERIFIED COMPLAINT UNDER
SECTION 337 OF THE TARIFF ACTION OF 1930**

COMPLAINANTS

RevoLaze, LLC
29300 Clemens Rd.
Westlake, OH 44145
Telephone: 440-617-0502

TechnoLines, LLC
29300 Clemens Rd.
Westlake, OH 44145
Telephone: 440-617-0502

COUNSEL FOR COMPLAINANTS

Mark L. Hogge
Shailendra K. Maheshwari
Steven J. Stein
Nicholas H. Jackson
DENTONS US LLP
1301 K Street, N.W.
6th Floor, East Tower
Washington, D.C. 20005
Telephone: 202.408.6400
Facsimile: 202.408.6399

PROPOSED RESPONDENTS

Abercrombie & Fitch Co.
6301 Fitch Path
New Albany, Ohio 43054
Telephone: 614-283-6500

American Eagle Outfitters, Inc.
77 Hot Metal Street
Pittsburgh, Pennsylvania 15203
Telephone: 412-432-3300

BBC Apparel Group, LLC
1407 Broadway
Suite 503
New York, New York 10018
Telephone: 212-997-0230

Gotham Licensing Group, LLC
1407 Broadway
Suite 506
New York, New York 10018

The Buckle, Inc.
2407 West 24th Street
Kearney, Nebraska 68845
Telephone: 800-626-1255

Buffalo International ULC
400 Sauve West
Montreal, Quebec H3L 1Z8
Canada
Telephone: 1-888-883-8710

1724982 Alberta ULC
400 Sauve West
Montreal, Quebec H3L1Z8
Canada
Telephone: 1-888-883-8710

Diesel S.p.A.
via dell'Industria, 4/6
36042 Breganze (VI)
Italy
Telephone: 00642650246
From U.S.: +01139.0642.265.0246

DL1961 Premium Denim Inc.
530 7th Avenue
Suite 1505
New York, New York 10018
Telephone: 646-514-9736, ext. 130

Eddie Bauer LLC
10401 NE 8th Street
Suite 500
Bellevue, Washington 98004
Telephone: 425-755-8100

The Gap, Inc.
2 Folsom Street
San Francisco, California 94105
Telephone: 415-427-0100

Guess?, Inc.
1444 South Alameda Street
Los Angeles, California 90021
Telephone: 213-765-5578

H&M Hennes & Mauritz AB
Mäster Samuelsgatan 46A
SE-106 38 Stockholm
Sweden
Telephone: +46 8 796 55 00

H&M Hennes & Mauritz LP
110 Fifth Avenue, 11th Floor
New York, New York 10011
Telephone: 212-564-9922

Roberto Cavalli S.p.A.
Piazza San Babila 3
20122 Milan
Italy
Telephone: +39 02 763 0771

Koos Manufacturing, Inc.
2741 Seminole Ave.
South Gate, CA 90280
Telephone: 323-564-2100

Levi Strauss & Co.
1155 Battery Street
San Francisco, California 94111
Telephone: 415-501-6000

Lucky Brand Dungarees, Inc.
540 S. Santa Fe Ave.
Los Angeles, CA 90013
Telephone: 213-443-5700

Fashion Box S.p.A.
Via Marcoui, 1
31011 Localita Casella
Asolo (Treviso)
Italy
Telephone: +39 0423 9251

VF Corporation
105 Corporate Center Blvd.
Greensboro, North Carolina 27408
Telephone: 336-424-6000

TABLE OF CONTENTS

	<u>Page</u>
LIST OF EXHIBITS.....	iii
LIST OF APPENDICES.....	xi
I. INTRODUCTION	1
II. THE PARTIES.....	2
A. Complainants	2
B. Proposed Respondents	4
III. THE PATENTS AT ISSUE.....	12
A. The '444 Patent – Laser Method and System of Scribing Graphics.....	12
B. The '602 Patent – Marking of Fabrics and Other Materials Using a Laser	12
C. The '196 Patent – Laser Method of Scribing Graphics	13
D. The '505 Patent – Laser Processing of Materials Using Mathematical Tools.....	13
E. The '972 Patent – Material Surface Processing with a Laser that has a Scan Modulated Effective Power to Achieve Multiple Worn Looks	14
F. The '815 Patent – Denim Designs from Laser Scribing	14
G. Foreign Counterparts	15
H. Licensees.....	16
I. Non-Technical Description of the Patented Technologies	16
IV. THE PRODUCTS AT ISSUE	18
A. Complainants Products	18
B. Respondent’s Infringing Products.....	18
V. UNLAWFUL AND UNFAIR ACTS OF THE RESPONDENTS	19
A. A&F	19
B. American Eagle Outfitters	20
C. BlankNYC.....	20
D. Buckle	21

- E. Buffalo 22
- F. [Reserved] 22
- G. Diesel 22
- H. DL1961 23
- I. Eddie Bauer 24
- J. Gap 24
- K. Guess? 25
- L. H&M 25
- M. Just Cavalli 26
- N. Koos 27
- O. Levi's 27
- P. Lucky 28
- Q. Replay 29
- R. VF Corp. 30
- VI. SPECIFIC INSTANCES OF IMPORTATION AND SALE 30
- VII. CLASSIFICATION OF THE INFRINGING PRODUCTS UNDER THE HARMONIZED TARIFF SCHEDULE OF THE UNITED STATES, 31
- VIII. RELATED LITIGATION 31
- IX. DOMESTIC INDUSTRY 32
 - A. Technical Prong 32
 - B. Economic Prong 34
- X. GENERAL EXCLUSION ORDER 35
- XI. RELIEF REQUESTED 36

Exhibit List		
Exhibit Number	Description	Designation
1	Certified Copies of the Asserted Patents	
A	U.S. Patent No. 5,990,444	Public
B	U.S. Patent No. 6,140,602	Public
C	U.S. Patent No. 6,252,196	Public
D	U.S. Patent No. 6,664,505	Public
E	U.S. Patent No. 6,819,972	Public
F	U.S. Patent No. 6,858,815	Public
2	Certified Assignment Records of the Asserted Patents	
A	Certified Assignment Record for U.S. Patent No. 5,990,444	Public
B	Certified Assignment Record for U.S. Patent No. 6,140,602	Public
C	Certified Assignment Record for U.S. Patent No. 6,252,196	Public
D	Certified Assignment Record for U.S. Patent No. 6,664,505	Public
E	Certified Assignment Record for U.S. Patent No. 6,819,972	Public
F	Certified Assignment Record for U.S. Patent No. 6,858,815	Public
3	Foreign Counterparts to Asserted Patents	
4	Licenses	
A	DVUV, LLC	Confidential
B	GST AutoLeather	Confidential
C	Lear Corp.	Confidential
D	Green Bay Decking, LLC	Confidential
5	Accused Products' Images	
A	A&F - Hollister Product	Public
B	American Eagle Product	Public
C	BlankNYC Product	Public
D	Buckle Product	Public
E	Buffalo Product	Public
F	[Reserved]	
G	Diesel Product	Public
H	DL1961 Product	Public
I	Eddie Bauer Product	Public
J	Gap Product	Public
K	Guess Product	Public
L	H&M Product	Public
M	Just Cavalli Product	Public
N	Koos - AG Jeans Product	Public
O	Koos - Big Star Product	Public

P	Levi's Product	Public
Q	Lucky Product	Public
R	Replay Product	Public
S	VF (Seven for All Mankind) Product	Public
6	Importation	
A	Ryan Ripley Declaration	Public
B	A&F - Hollister Receipt	Public
C	American Eagle Receipt	Public
D	BlankNYC Receipt	Public
E	Buckle Receipt	Public
F	Buffalo Receipt	Public
G	[Reserved]	
H	Diesel Receipt	Public
I	DL1961 Receipt	Public
J	Eddie Bauer Receipt	Public
K	Gap Receipt	Public
L	Guess Receipt	Public
M	H&M Receipt	Public
N	Just Cavalli Receipt	Public
O	Koos - AG Jeans Receipt	Public
P	Koos - Big Star Receipt	Public
Q	Levi's Receipt	Public
R	Lucky Receipt	Public
S	Replay Receipt	Public
T	VF (Seven For All Mankind) Receipt	Public
7	Claim Analysis Against Accused Products	
A	Marcatex Flexi Manual Rev 1.3.1 _English_ FDA	Public
B	YouTube Video – Jeanologia, Flexi3 ONE MACHINE, MULTIPLE OPTIONS (https://www.youtube.com/watch?v=apPFfm78_1E&feature=c4-overview&list=UUXQ2v180qUHLWKYzvGkNMQg)	Public
C	YouTube Video – Jeanologia, Laser System_ Twin HS at Itma Barcelona 2011 (https://www.youtube.com/watch?v=CSP_ZxgIQQI)	Public
D	YouTube Video – Tonello, Laser Blaze by Tonello (https://www.youtube.com/watch?v=a2BJiDM8kpg)	Public
E	YouTube Video – Macsa ID, S.A., DENIM - LASERTEX Pro - Macsa Laser Systems (https://www.youtube.com/watch?v=IDAt9dcSMv8)	Public

F	YouTube Video – Jeanologia, Laser Technology in Siete Leguas (https://www.youtube.com/watch?v=8u4WPumH6Kg)	Public
G	YouTube Video – Jeanologia, Finishing Jeans Present And Future Trends And Technologies In Denim 02 (http://www.youtube.com/watch?v=HgxvoYgl-tM)	Public
H	YouTube Video – Replay Laserblast	Public
I	YouTube Video – Replay Laserblast - Official Teaser	Public
J	CBS This Morning, Levi’s New Stadium – Brand launches \$1.2 billion sports arena	Public
8	Abercrombie Claim Charts	
A	Abercrombie Claim Chart U.S. Patent 5,990,444	Public
B	Abercrombie Claim Chart U.S. Patent 6,140,602	Public
C	Abercrombie Claim Chart U.S. Patent 6,252,196	Public
D	Abercrombie Claim Chart U.S. Patent 6,664,505	Public
E	Abercrombie Claim Chart U.S. Patent 6,819,972	Public
F	Abercrombie Claim Chart U.S. Patent 6,858,815	Public
9	American Eagle Claim Charts	
A	American Eagle Claim Chart U.S. Patent 5,990,444	Public
B	American Eagle Claim Chart U.S. Patent 6,140,602	Public
C	American Eagle Claim Chart U.S. Patent 6,252,196	Public
D	American Eagle Claim Chart U.S. Patent 6,664,505	Public
E	American Eagle Claim Chart U.S. Patent 6,819,972	Public
F	American Eagle Claim Chart U.S. Patent 6,858,815	Public
10	BlankNYC Claim Charts	
A	BlankNYC Claim Chart U.S. Patent 5,990,444	Public
B	BlankNYC Claim Chart U.S. Patent 6,140,602	Public
C	BlankNYC Claim Chart U.S. Patent 6,252,196	Public
D	BlankNYC Claim Chart U.S. Patent 6,664,505	Public
E	BlankNYC Claim Chart U.S. Patent 6,819,972	Public
F	BlankNYC Claim Chart U.S. Patent 6,858,815	Public
11	Buckle Claim Charts	
A	Buckle Claim Chart U.S. Patent 5,990,444	Public
B	Buckle Claim Chart U.S. Patent 6,140,602	Public
C	Buckle Claim Chart U.S. Patent 6,252,196	Public
D	Buckle Claim Chart U.S. Patent 6,664,505	Public
E	Buckle Claim Chart U.S. Patent 6,819,972	Public
F	Buckle Claim Chart U.S. Patent 6,858,815	Public
12	Buffalo Claim Charts	
A	Buffalo Claim Chart U.S. Patent 5,990,444	Public
B	Buffalo Claim Chart U.S. Patent 6,140,602	Public

C	Buffalo Claim Chart U.S. Patent 6,252,196	Public
D	Buffalo Claim Chart U.S. Patent 6,664,505	Public
E	Buffalo Claim Chart U.S. Patent 6,819,972	Public
F	Buffalo Claim Chart U.S. Patent 6,858,815	Public
13	[Reserved]	
14	Diesel Claim Charts	
A	Diesel Claim Chart U.S. Patent 5,990,444	Public
B	Diesel Claim Chart U.S. Patent 6,140,602	Public
C	Diesel Claim Chart U.S. Patent 6,252,196	Public
D	Diesel Claim Chart U.S. Patent 6,664,505	Public
E	Diesel Claim Chart U.S. Patent 6,819,972	Public
F	Diesel Claim Chart U.S. Patent 6,858,815	Public
15	DL1961 Claim Charts	
A	DL1961 Claim Chart U.S. Patent 5,990,444	Public
B	DL1961 Claim Chart U.S. Patent 6,140,602	Public
C	DL1961 Claim Chart U.S. Patent 6,252,196	Public
D	DL1961 Claim Chart U.S. Patent 6,664,505	Public
E	DL1961 Claim Chart U.S. Patent 6,819,972	Public
F	DL1961 Claim Chart U.S. Patent 6,858,815	Public
16	Eddie Bauer Claim Charts	
A	Eddie Bauer Claim Chart U.S. Patent 5,990,444	Public
B	Eddie Bauer Claim Chart U.S. Patent 6,140,602	Public
C	Eddie Bauer Claim Chart U.S. Patent 6,252,196	Public
D	Eddie Bauer Claim Chart U.S. Patent 6,664,505	Public
E	Eddie Bauer Claim Chart U.S. Patent 6,819,972	Public
F	Eddie Bauer Claim Chart U.S. Patent 6,858,815	Public
17	Gap Claim Charts	
A	Gap Claim Chart U.S. Patent 5,990,444	Public
B	Gap Claim Chart U.S. Patent 6,140,602	Public
C	Gap Claim Chart U.S. Patent 6,252,196	Public
D	Gap Claim Chart U.S. Patent 6,664,505	Public
E	Gap Claim Chart U.S. Patent 6,819,972	Public
F	Gap Claim Chart U.S. Patent 6,858,815	Public
18	Guess Claim Charts	
A	Guess Claim Chart U.S. Patent 5,990,444	Public
B	Guess Claim Chart U.S. Patent 6,140,602	Public
C	Guess Claim Chart U.S. Patent 6,252,196	Public
D	Guess Claim Chart U.S. Patent 6,664,505	Public
E	Guess Claim Chart U.S. Patent 6,819,972	Public

	F	Guess Claim Chart U.S. Patent 6,858,815	Public
19	H&M Claim Charts		
	A	H&M Claim Chart U.S. Patent 5,990,444	Public
	B	H&M Claim Chart U.S. Patent 6,140,602	Public
	C	H&M Claim Chart U.S. Patent 6,252,196	Public
	D	H&M Claim Chart U.S. Patent 6,664,505	Public
	E	H&M Claim Chart U.S. Patent 6,819,972	Public
	F	H&M Claim Chart U.S. Patent 6,858,815	Public
20	Just Cavalli Claim Charts		
	A	Just Cavalli Claim Chart U.S. Patent 5,990,444	Public
	B	Just Cavalli Claim Chart U.S. Patent 6,140,602	Public
	C	Just Cavalli Claim Chart U.S. Patent 6,252,196	Public
	D	Just Cavalli Claim Chart U.S. Patent 6,664,505	Public
	E	Just Cavalli Claim Chart U.S. Patent 6,819,972	Public
	F	Just Cavalli Claim Chart U.S. Patent 6,858,815	Public
21	Koos – The Matchbox (AG Jeans) Claim Charts		
	A	Koos - The Matchbox (AG Jeans) Claim Chart U.S. Patent 5,990,444	Public
	B	Koos - The Matchbox (AG Jeans) Claim Chart U.S. Patent 6,140,602	Public
	C	Koos - The Matchbox (AG Jeans) Claim Chart U.S. Patent 6,252,196	Public
	D	Koos - The Matchbox (AG Jeans) Claim Chart U.S. Patent 6,664,505	Public
	E	Koos - The Matchbox (AG Jeans) Claim Chart U.S. Patent 6,819,972	Public
	F	Koos - The Matchbox (AG Jeans) Claim Chart U.S. Patent 6,858,815	Public
22	Koos – Big Star Claim Charts		
	A	Koos - Big Star Claim Chart U.S. Patent 5,990,444	Public
	B	Koos - Big Star Claim Chart U.S. Patent 6,140,602	Public
	C	Koos - Big Star Claim Chart U.S. Patent 6,252,196	Public
	D	Koos - Big Star Claim Chart U.S. Patent 6,664,505	Public
	E	Koos - Big Star Claim Chart U.S. Patent 6,819,972	Public
	F	Koos - Big Star Claim Chart U.S. Patent 6,858,815	Public
23	Levi's Claim Charts		
	A	Levi's Claim Chart U.S. Patent 5,990,444	Public
	B	Levi's Claim Chart U.S. Patent 6,140,602	Public
	C	Levi's Claim Chart U.S. Patent 6,252,196	Public

D	Levi's Claim Chart U.S. Patent 6,664,505	Public
E	Levi's Claim Chart U.S. Patent 6,819,972	Public
F	Levi's Claim Chart U.S. Patent 6,858,815	Public
24	Lucky Brand Claim Charts	
A	Lucky Brand Claim Chart U.S. Patent 5,990,444	Public
B	Lucky Brand Claim Chart U.S. Patent 6,140,602	Public
C	Lucky Brand Claim Chart U.S. Patent 6,252,196	Public
D	Lucky Brand Claim Chart U.S. Patent 6,664,505	Public
E	Lucky Brand Claim Chart U.S. Patent 6,819,972	Public
F	Lucky Brand Claim Chart U.S. Patent 6,858,815	Public
25	Replay Claim Charts	
A	Replay Claim Chart U.S. Patent 5,990,444	Public
B	Replay Claim Chart U.S. Patent 6,140,602	Public
C	Replay Claim Chart U.S. Patent 6,252,196	Public
D	Replay Claim Chart U.S. Patent 6,664,505	Public
E	Replay Claim Chart U.S. Patent 6,819,972	Public
F	Replay Claim Chart U.S. Patent 6,858,815	Public
26	VF Corp. Claim Charts	
A	VF Claim Chart U.S. Patent 5,990,444	Public
B	VF Claim Chart U.S. Patent 6,140,602	Public
C	VF Claim Chart U.S. Patent 6,252,196	Public
D	VF Claim Chart U.S. Patent 6,664,505	Public
E	VF Claim Chart U.S. Patent 6,819,972	Public
F	VF Claim Chart U.S. Patent 6,858,815	Public
	Domestic Industry	
27	Linear Processing Claim Charts	
A	Linear Processing Claim Chart for U.S. Patent No. 5,990,444	Confidential
B	Linear Processing Claim Chart for U.S. Patent No. 6,140,602	Confidential
C	Linear Processing Claim Chart for U.S. Patent No. 6,252,196	Confidential
D	Linear Processing Claim Chart for U.S. Patent No. 6,664,505	Confidential
E	Linear Processing Claim Chart for U.S. Patent No. 6,819,972	Confidential
F	Linear Processing Claim Chart for U.S. Patent No. 6,858,815	Confidential
G	Video - RevoLaze Linear Processing	Public
28	Sports Logos Claim Charts	
A	Sport Logos Claim Chart for U.S. Patent No. 5,990,444	Confidential
B	Sport Logos Claim Chart for U.S. Patent No. 6,140,602	Confidential
C	Sport Logos Claim Chart for U.S. Patent No. 6,252,196	Confidential
D	Sport Logos Claim Chart for U.S. Patent No. 6,664,505	Confidential
E	Sport Logos Claim Chart for U.S. Patent No. 6,819,972	Confidential

F	Sport Logos Claim Chart for U.S. Patent No. 6,858,815	Confidential
G	Video - Chicago Bears Logo	Confidential
29	Terrain (Green Bay Decking) Claim Charts	
A	Terrain Claim Chart for U.S. Patent No. 5,990,444	Confidential
B	Terrain Claim Chart for U.S. Patent No. 6,140,602	Confidential
C	Terrain Claim Chart for U.S. Patent No. 6,252,196	Confidential
D	Terrain Claim Chart for U.S. Patent No. 6,664,505	Confidential
E	Terrain Claim Chart for U.S. Patent No. 6,819,972	Confidential
F	Terrain Claim Chart for U.S. Patent No. 6,858,815	Confidential
G	Video - Plastic Lumber	Public
30	Cloth Upholstery (Lear Corp.) Claim Charts	
A	Cloth Upholstery Claim Chart for U.S. Patent No. 5,990,444	Confidential
B	Cloth Upholstery Claim Chart for U.S. Patent No. 6,140,602	Confidential
C	Cloth Upholstery Claim Chart for U.S. Patent No. 6,252,196	Confidential
D	Cloth Upholstery Claim Chart for U.S. Patent No. 6,664,505	Confidential
E	Cloth Upholstery Claim Chart for U.S. Patent No. 6,819,972	Confidential
F	Cloth Upholstery Claim Chart for U.S. Patent No. 6,858,815	Confidential
G	Cloth Upholstery Video	Confidential
31	Leather Upholstery (GST AutoLeather) Claim Charts	
A	Leather Upholstery Claim Chart for U.S. Patent No. 5,990,444	Confidential
B	Leather Upholstery Claim Chart for U.S. Patent No. 6,140,602	Confidential
C	Leather Upholstery Claim Chart for U.S. Patent No. 6,252,196	Confidential
D	Leather Upholstery Claim Chart for U.S. Patent No. 6,664,505	Confidential
E	Ram Adds New Laramie Longhorn, Outdoorsman Models to 2600/3500 Heavy Duty Lineup (Sep. 14, 2010)	Public
F	2013 Dodge Ram 1500 Brochure	Public
32	DVUV Claim Charts	
A	DVUV Claim Chart for U.S. Patent No. 5,990,444	Confidential
B	DVUV Claim Chart for U.S. Patent No. 6,140,602	Confidential
C	DVUV Claim Chart for U.S. Patent No. 6,252,196	Confidential
D	DVUV Claim Chart for U.S. Patent No. 6,664,505	Confidential
E	DVUV Claim Chart for U.S. Patent No. 6,858,815	Confidential
F	DVUV Video	Confidential
G	DVUV Cutting Shop Manual	Public
33	High Speed Abrasion Claim Charts	
A	High Speed Abrasion Claim Chart for U.S. Patent No. 5,990,444	Confidential
B	High Speed Abrasion Claim Chart for U.S. Patent No. 6,140,602	Confidential
C	High Speed Abrasion Claim Chart for U.S. Patent No. 6,252,196	Confidential
D	High Speed Abrasion Claim Chart for U.S. Patent No. 6,664,505	Confidential
E	High Speed Abrasion Claim Chart for U.S. Patent No. 6,819,972	Confidential

F	High Speed Abrasion Claim Chart for U.S. Patent No. 6,858,815	Confidential
G	High Speed Abrasion Taylor Togs Video	Public
H	High Speed Abrasion VF Jeanswear Video	Public
34	Darryl J. Costin, Ph.D. Domestic Industry Declaration	
A	Declaration of Darryl J. Costin, Ph.D.	Confidential
B	Laser Demonstration and Launch Party Video	Public
C	Video - Coach Sports Jeans	Public
D	Textile Roll Goods Brochure	Public
E	Video - Textile Roll Goods	Public
F	Confidentiality and Non-Disclosure Agreement by and between Struktol Company of America and RevoLaze, LLC	Confidential
G	RevoLaze/Cone Denim Non-Disclosure Agreement	Confidential
35	News Articles and Publications	
A	Jeanologia Seeking a Friendlier Denim Finish	Public
B	Jeanologia: Ultimate Technology for Jean Finishing	Public
C	Easy Laser - Our Customers	Public
D	fibre 2 fashion - Jeanologia dominates Mexican garment finishing market	Public
E	Jeanologia's lead in sustainable technology for garment finishing	Public
F	WWD - Panel: Industry Drives Sustainability Effort	Public
G	Koos - Ocean Bill of Lading	Public
H	Levi Strauss & Co., Environment, Health and Safety Handbook	Public
I	Bobbin, TechnoLines Debuts Laser Applications for Fabric Scribing, Sandblasting	Public
J	Laser Scribes Out Fabric Designs - Automotive Engineering	Public
	Technical Declarations	
36	Darryl J. Costin, Ph.D. Technical Declaration	
A	Declaration of Darryl J. Costin, Ph.D.	Public
B	Costin Resume	Confidential
C	Chow et al., Effect of CO2 laser treatment on cotton surface, 18 Cellulose 1635	Public
D	Table - energy density per unit area per unit time (EDPUT)	Public
37	William Murcia Technical Declaration	
A	Declaration of William Murcia	Confidential
B	Murcia Resume	Public

Appendices List		
Appendix	Description	Designation
	Certified File Wrappers and Cited References	
A	Certified File Wrapper for U.S. Patent No. 5,990,444	Public
B	Cited References for U.S. Patent No. 5,990,444	Public
C	Certified File Wrapper for U.S. Patent No. 6,140,602	Public
D	Cited References for U.S. Patent No. 6,140,602	Public
E	Certified File Wrapper for U.S. Patent No. 6,252,196	Public
F	Cited References for U.S. Patent No. 6,252,196	Public
G	Certified File Wrapper for U.S. Patent No. 6,664,505	Public
H	Cited References for U.S. Patent No. 6,664,505	Public
I	Certified File Wrapper for U.S. Patent No. 6,819,972	Public
J	Cited References for U.S. Patent No. 6,819,972	Public
K	Certified File Wrapper for U.S. Patent No. 6,858,815	Public
L	Cited References for U.S. Patent No. 6,858,815	Public

I. INTRODUCTION

1. This Complaint is filed, pursuant to Section 337 of the Tariff Act of 1930 as amended (19 U.S.C. § 1337), by RevoLaze, LLC (“RevoLaze”) and TechnoLines, LLC (“TechnoLines”) (collectively “Complainants”) based on unfair methods of competition and unfair acts in the unlawful importation into the United States, sale for importation into the United States, or sale within the United States after importation by Abercrombie & Fitch Co.; American Eagle Outfitters, Inc.; BBC Apparel Group, LLC; Gotham Licensing Group, LLC; The Buckle, Inc.; Buffalo International ULC; 1724982 Alberta ULC; Diesel S.p.A.; DL1961 Premium Denim Inc.; Eddie Bauer LLC; The Gap, Inc.; Guess?, Inc.; H&M Hennes & Mauritz AB; H&M Hennes & Mauritz LP; Roberto Cavalli S.p.A. d/b/a Just Cavalli; Koos Manufacturing, Inc. d/b/a AG Jeans and Big Star; Levi Strauss & Co.; Lucky Brand Dungarees, Inc.; Fashion Box S.p.A. d/b/a Replay Jeans; and VF Corporation d/b/a 7 for All Mankind (collectively “Respondents”) of certain laser abraded denim garments (collectively the “Accused Products”). The Accused Products manufactured, imported, offered for sale, and/or sold by Respondents are manufactured by methods directly infringing, under 19 U.S.C. § 1337(a)(1)(B)(ii), one or more claims (the “Asserted Claims”) of the following U.S. patents (the “Asserted Patents” or “Patents-in-Suit”) owned by RevoLaze.

- Claims 1-3, 8, 21, 33-34, 46, 69, 70, and 72 of U.S. Patent No. 5,990,444 (“the ’444 Patent”) (“Exhibit 1A”);
- Claims 1, 14, 15, 53, 73, 83, 85, 94, 97, 99, 112, 120, 122-125, and 141-143 of U.S. Patent No. 6,140,602 (“the ’602 Patent”) (“Exhibit 1B”);
- Claims 5, 11, 13, 14, and 16 of U.S. Patent No. 6,252,196 (“the ’196 Patent”) (“Exhibit 1C”);

- Claims 1 and 49-51 of U.S. Patent No. 6,664,505 (“the ’505 Patent”) (“Exhibit 1D”);
- Claims 1, 2, 4-6, 11, 12, 16-19, 56-59, 61, 63, 64, 72, 77, 78, 83-87, and 92-95 of U.S. Patent No. 6,819,972 (“the ’972 Patent”) (“Exhibit 1E”); and
- Claims 13 and 14 of U.S. Patent No. 6,858,815 (“the ’815 Patent”) (“Exhibit 1F”).

2. Complainants seek a permanent general exclusion order barring infringing denim garments from entry into the United States. In the alternative, Complainants seek a limited exclusion order barring the infringing denim garments manufactured by or on the behalf of Respondents and are imported, offered for sale, sold, sold for importation, or sold after importation by Respondents. Complainants also seek permanent cease-and-desist orders against each Respondent prohibiting the importation, sale, offer for sale, advertisement, or solicitation of any sale by Respondents of the Accused Products or other products encompassed by the claims of the Patents-in-Suit.

II. **THE PARTIES**

A. **Complainants**

3. RevoLaze, LLC is a Delaware limited liability company with its principal place of business at 29300 Clemens Road, Westlake, Ohio 44145. TechnoLines, LLC, a Delaware limited liability company with the same address, is the majority member of RevoLaze and invested some 20 years in the research, development, obtainment of numerous patents and commercialization of its novel laser scribing technology. Through the use of sophisticated mathematical modeling techniques, TechnoLines overcame the technical barriers to successfully laser scribe high quality graphics and patterns on a host of textile fabrics including denim, cotton, polyester, nylon, and silk, as well as vinyl, suede, and leather.

4. Complainants have made a significant long-term investment to build the textile laser scribing technology business in the United States. They have dedicated considerable technical manpower, research and development facilities (three in Ohio and one in Minnesota) and financial resources for the invention and commercialization of their unique laser scribing technology to impart graphics and patterns on myriad of substrates. Importantly, Complainants' technology answers the textile industry's cry for sustainability, eco-friendliness and is in perfect alignment with the green movement for the environment.

5. Over the course of the last 15 years, Complainants have developed the technology and associated equipment through licensing with garment manufacturers including Sights Denim Systems, Taylor Togs, Inc., VF Corporation, Gear For Sports, Inc., and Final Finish Laundry. None of these licenses is still in force. Complainants' subsidiaries also previously operated two denim jean companies offering denim apparel manufactured by the patented technology: Fractal Jean Co. and Fins Denim Co.

6. Complainants' laser abrasion technology replaces the extremely dangerous and harmful sandblasting process, which has been found to be associated with a disabling lung disease called silicosis, to create a worn look on denim jeans. Because silicosis may result in death to workers, numerous denim jean companies, including industry leaders, have banned the use of sandblasting. Complainants, through the use of their 2,500-Watt laser systems, offer a patented laser abrading technology to solve this catastrophic health problem and substantially increase throughput versus the sandblast process.

7. Complainants also have introduced linear processing technology to the market that may revolutionize the textile industry by reducing the environmental impact associated with processes like enzyme washing jeans. A worldwide concern exists regarding the

environmental hazards associated with enzyme washing jeans and other processes such as the environmentally burdensome chemical printing processes that is used to laser scribe graphics and patterns to denim jeans. Complainants' linear laser etching technology may reduce or eliminate these environmental problems.

8. Through a combination of software developed by Complainants and specifically designed material delivery systems, Complainants have created the highest speed, highest power galvanometric driven laser machines in the industry that can economically apply graphics and patterns on fabrics and other substrates. Complainants continue to invest in developing new concepts for laser scribing materials in unique ways to solve current environmental, quality and cost problems associated with manufacturing and decorating garments and textiles.

9. RevoLaze is the owner of each of the Patents-in-Suit. Exhibits 2A-2F.

B. Proposed Respondents

10. Abercrombie & Fitch Co. ("A&F") d/b/a Hollister Jeans is a Delaware corporation with its principal place of business at 6301 Fitch Path, New Albany, Ohio 43054. On information and belief, A&F makes in Guatemala, has others make in Guatemala, exports from Guatemala into the United States, and imports from Guatemala certain denim garments that are made by methods that are claimed in the Patents-in-Suit. A&F also operates multiple retail stores across the United States under both the Hollister brand and the Abercrombie & Fitch brand. *See* Abercrombie & Fitch Store Locator, <http://www.abercrombie.com/webapp/wcs/stores/servlet/StoreLocator?catalogId=10901&langId=-1&storeId=10051> (last visited July 14, 2014); Hollister Co. Store Locator, <http://www.hollisterco.com/webapp/wcs/stores/servlet/StoreLocator?catalogId=10201&langId=->

1&storeId=10251 (last visited July 14, 2014). Specifically, A&F sells to retail customers and/or wholesalers within the United States imported, infringing garments including the Hollister High Rise Super Skinny – Medium Jeans (Item No. 355-550-0184-024) (“A&F Product”). A sample of the A&F Product is shown in Exhibit 5A.

11. American Eagle Outfitters, Inc. (“AEO”) is a Delaware corporation with its principal place of business at 77 Hot Metal Street, Pittsburgh, Pennsylvania 15203. On information and belief, AEO makes in Mexico, has others make in Mexico, exports from Mexico into the United States, and imports from Mexico certain denim garments that are made by methods that are claimed in the Patents-in-Suit. AEO also operates multiple retail stores across the United States. American Eagle Outfitters Store Locator, <http://www.ae.com/web/storelocator/default.jsp> (last visited July 15, 2014). Specifically, AEO sells to retail customers and/or wholesalers within the United States imported, infringing garments including the American Eagle Men’s Original Straight – Dark Tinted Crackle Jeans (Item No. 2870) (“AEO Product”). A sample of the AEO Product is shown in Exhibit 5B.

12. BBC Apparel Group, LLC and Gotham Licensing Group, LLC d/b/a BlankNYC (collectively “BlankNYC”) are companies with their principal place of business at 1407 Broadway, New York, New York 10018. BlankNYC has a business address at 275 West 39th Street, New York, New York 10018. On information and belief, BlankNYC makes in China, has others make in China, exports from China into the United States, and imports from China certain denim garments that are made by methods that are claimed in the Patents-in-Suit. Specifically, BlankNYC sells to retail customers and/or wholesalers within the United States imported, infringing garments including the BlankNYC Polka Dot Jeans (“BlankNYC Product”). A sample of the BlankNYC Product is shown in Exhibit 5C.

13. The Buckle, Inc. (“Buckle”) is a Nebraska corporation with its principal place of business at 2407 West 24th Street, Kearney, Nebraska 68845. On information and belief, Buckle makes in Mexico, has others make in Mexico, exports from Mexico into the United States, and imports from Mexico certain denim garments that are made by methods that are claimed in the Patents-in-Suit. Buckle also operates multiple retail stores across the United States. Buckle Store Locator, <http://www.buckle.com/stores/locator.jsp;jsessionid=hDJGTFHTsYlg6gkNBn9nhBbjGHGgnn3kGNvkrvcvGnn8v2YKk2Wy!-2113174839!-695411156> (last visited July 15, 2014). Specifically, Buckle sells to retail customers and/or wholesalers within the United States imported, infringing products including the Buckle BKE Payton Bootcut – Porter Jeans (Item No. BPL1403L) (“Buckle Product”). A sample of the Buckle Product is shown in Exhibit 5D.

14. Buffalo International ULC and 1724982 Alberta ULC d/b/a Buffalo David Bitton (collectively “Buffalo”) are Quebec companies with business addresses at 400 Sauve West, Montreal, Quebec H3L 1Z8. On information and belief, Buffalo makes in Thailand, has others make in Thailand, exports from Thailand into the United States, and imports from Thailand certain denim garments that are made by methods that are claimed in the Patents-in-Suit. Specifically, Buffalo sells to retail customers and/or wholesalers within the United States imported, infringing garments including the Buffalo Driven-X (Item No. BM16324) (“Buffalo Product”). A sample of the Buffalo Product is shown in Exhibit 5E.

15. [Reserved].

16. Diesel S.p.A. (“Diesel”) is an Italian company with its principal place of business at via dell’Industria, 4/6, 36042 Breganze (VI), Italy. On information and belief, Diesel makes in Italy, has others make in Italy, exports from Italy into the United States, and imports

from Italy certain denim garments that are made by methods that are claimed in the Patents-in-Suit. Diesel also operates multiple stores across the United States. *See* Diesel Store Locator, www.diesel.com/store-locator (last visited July 14, 2014). Specifically, Diesel sells to retail customers and/or wholesalers within the United States imported, infringing garments including Diesel Shioner Skinny Fit Jeans (Item No. 117009) (“Diesel Product”). A sample of the Diesel Product is shown in Exhibit 5G.

17. DL1961 Premium Denim Inc. (“DL1961”) is a Delaware corporation with its principal place of business at 530 7th Avenue, Suite 1505, New York, New York 10018. On information and belief, DL1961 makes in Pakistan, has others make in Pakistan, exports from Pakistan into the United States, and imports from Pakistan certain denim garments that are made by methods that are claimed in the Patents-in-Suit. Specifically, DL1961 sells to retail customers and/or wholesalers within the United States imported, infringing garments including the DL1961 Emma Legging – McCarren (No. 2264) (“DL1961 Product”). A sample of the DL1961 Product is shown in Exhibit 5H.

18. Eddie Bauer LLC (“Eddie Bauer”) is a Delaware limited liability company with its principal place of business at 10401 NE 8th Street, Suite 500, Bellevue, Washington 98004. On information and belief, Eddie Bauer makes in Sri Lanka, has others make in Sri Lanka, exports from Sri Lanka into the United States, and imports from Sri Lanka certain denim garments that are made by methods that are claimed in the Patents-in-Suit. Eddie Bauer also operates multiple retail stores across the United States. Eddie Bauer Store Locator, http://www.eddiebauer.com/storelocator/store_locator.jsp? (last visited July 15, 2014). Specifically, Eddie Bauer sells to retail customers and/or wholesalers within the United States

imported, infringing garments including the Eddie Bauer Skinny Print Jeans (Style No. 2974) (“Eddie Bauer Product”). A sample of the Eddie Bauer Product is shown in Exhibit 5I.

19. The Gap, Inc. (“Gap”) is a Delaware corporation with its principal place of business at 2 Folsom Street, San Francisco, California 94105. On information and belief, Gap makes in China, has others make in China, exports from China into the United States, and imports from China certain denim garments that are made by methods that are claimed in the Patents-in-Suit. Gap also operates multiple retail stores across the United States. *See* Gap Store Locator, <http://www.gap.com/customerService/storeLocator.do?mlink=39813,6836749,StoreLocator&mlink=6836749> (last visited July 14, 2014). Specifically, Gap sells to retail customers and/or wholesalers within the United States imported, infringing garments including the Gap Floral Print Always Skinny Jeans (Item No. 600542) (“Gap Product”). A sample of the Gap Product is shown in Exhibit 5J.

20. Guess?, Inc. (“Guess?”) is a Delaware corporation with its principal place of business at 1444 South Alameda Street, Los Angeles, California 90021. On information and belief, Guess? makes in Mexico, has others make in Mexico, exports from Mexico into the United States, and imports from Mexico certain denim garments that are made by methods that are claimed in the Patents-in-Suit. Guess? also operates multiple retail stores across the United States. Guess? Store Locator, shop.guess.com/en/StoreLocator (last visited July 14, 2014). Specifically, Guess? sells to retail customers and/or wholesalers within the United States imported, infringing products including Guess? Alameda Slim Fit Shorts – Hickory Wash (Style No. M41A01D1A91) (“Guess? Product”). A sample of the Guess? Product is shown in Exhibit 5K.

21. H&M Hennes & Mauritz AB is a Swedish company with its principal place of business at Mäster Samuelsgatan 46A, SE-106 38 Stockholm, Sweden. H&M Hennes & Mauritz LP is a New York company with a business address at 110 Fifth Avenue, 11th Floor, New York, New York 10011. H&M Hennes & Mauritz AB and H&M Hennes & Mauritz LP are collectively referred to as “H&M.” On information and belief, H&M makes in Turkey, has others make in Turkey, exports from Turkey into the United States, and imports from Turkey certain denim garments that are made by methods that are claimed in the Patents-in-Suit. H&M also operates multiple stores across the United States. *See* H&M Store Locator, <http://www.hm.com/us/store-locator> (last visited July 15, 2014). Specifically, H&M sells to retail customers and/or wholesalers within the United States imported, infringing garments including the H&M Boyfriend Low Waist Tapered Leg (“H&M Product”). A sample of the H&M Product is shown in Exhibit 5L.

22. Roberto Cavalli S.p.A. d/b/a Just Cavalli (“Just Cavalli”) is an Italian company with its principal place of business at Piazza San Babila 3 - 0122 Milan, Italy. On information and belief, Just Cavalli makes in Romania, has others make in Romania, exports from Romania into the United States, and imports from Romania certain denim garments that are made by methods that are claimed in the Patents-in-Suit. Just Cavalli operates two retail stores, one at One Borgata Way, Atlantic City, New Jersey, and a second at 434 West Broadway, New York, New York. Roberto Cavalli Store Locator, http://www.robortocavalli.com/store_locator/ (last visited July 15, 2014). Specifically, Just Cavalli sells to retail customers and/or wholesalers within the United States imported, infringing garments including the Just Cavalli Laser Croc Denim Shirt (“Just Cavalli Product”). A sample of the Just Cavalli Product is shown in Exhibit 5M.

23. Koos Manufacturing, Inc. d/b/a AG Jeans and Big Star Jeans (“Koos”) is a California corporation with its principal place of business at 2741 Seminole Avenue, South Gate, California 90280. On information and belief, Koos makes in Mexico, has others make in Mexico, exports from Mexico into the United States, and imports from Mexico certain denim garments that are made by methods that are claimed in the Patents-in-Suit. Koos also operates multiple retail stores across the United States under the AG Adriano Goldschmied name. AG Jeans Store Locator, <http://www.agjeans.com/store/storelocator.aspx> (last visited July 15, 2014). Specifically, Koos sells to retail customers and/or wholesalers within the United States imported, infringing garments including the AG Jeans, The Matchbox – Skinny Straight LON (Style No. 11311MALON) and the Big Star – Alex Skinny Pattern Jeans (Style No. SWALXFS) (collectively “Koos Products”). Samples of the Koos Products are shown in Exhibit 5N and 5O.

24. Levi Strauss & Co. (“Levi’s”) is a Delaware corporation with its principal place of business at 1155 Battery Street, San Francisco, California. On information and belief, Levi’s makes in Mexico, has others make in Mexico, exports from Mexico into the United States, and imports from Mexico certain denim garments that are made by methods that are claimed in the Patents-in-Suit. Levi’s also operates multiple stores across the United States. See Levi’s Store Locator, us.levi.com/storeLocator/ (last visited July 14, 2014). Specifically, Levi’s sells to retail customers and/or wholesalers within the United States imported, infringing garments including Levi’s 501 Original Fit Broken Black (Item No. 005011480) (“Levi’s Product”). A sample of the Levi’s Product is shown in Exhibit 5P.

25. Lucky Brand Dungarees, Inc. (“Lucky”) is a Delaware corporation with its principal place of business at 540 South Santa Fe Avenue, Los Angeles, California 90013. On information and belief, Lucky makes in Mexico, has others make in Mexico, exports from

Mexico into the United States, and imports from Mexico certain denim garments that are made by methods that are claimed in the Patents-in-Suit. Lucky also operates multiple retail stores across the United States. Lucky Brand Store Locator, <http://www.luckybrand.com/stores> (last visited July 15, 2014). Specifically, Lucky sells to retail customers and/or wholesalers within the United States imported, infringing garments including the Lucky Brand 363 New Vintage Straight Jeans (Style No. 7M11649) (“Lucky Product”). A sample of the Lucky Product is shown in Exhibit 5Q.

26. Fashion Box S.p.A. d/b/a Replay Jeans (“Replay”) is an Italian company with its principal place of business at Via Marcouli 1 - 31011 Localita Casella, Asolo (Treviso) Italy. On information and belief, Replay makes in Tunisia, has others make in Tunisia, exports from Tunisia into the United States, and imports from Tunisia certain denim garments that are made by methods that are claimed in the Patents-in-Suit. On information and belief, Replay previously operated retail stores at 860 Collins Avenue, Miami Beach, Florida 33139 and 109 Prince Street, New York, New York 10012. Specifically, Replay sells to retail customers and/or wholesalers within the United States imported, infringing garments including the Replay Re-Army 335 906 – Slim Bootcut Fit Jeans (Item Number WV676.000.335 906) (“Replay Product”). A sample of the Replay Product is shown in Exhibit 5R.

27. VF Corporation d/b/a 7 for All Mankind (“VF”) is a Pennsylvania corporation with its principal place of business at 105 Corporate Center Boulevard, Greensboro, North Carolina 27408. On information and belief, VF makes in Mexico, has others make in Mexico, exports from Mexico into the United States, and imports from Mexico certain denim garments that are made by methods that are claimed in the Patents-in-Suit. VF also operates multiple stores in the United States under the 7 for All Mankind name. 7 for All Mankind Store

Locator, <https://www.7forallmankind.com/store/storelocator.aspx> (last visited July 15, 2014).

Specifically, VF sells to retail customers and/or wholesalers within the United States imported, infringing garments including the Seven for All Mankind Austyn Jeans (Item No. JTA046702S) (“VF Product”). A sample of the VF Product is shown in Exhibit 5S.

III. THE PATENTS AT ISSUE

A. The '444 Patent – Laser Method and System of Scribing Graphics

28. The '444 Patent, entitled “Laser Method and System of Scribing Graphics,” was issued to Costin on November 23, 1999. A certified copy of the '444 Patent is attached to the Complaint as Exhibit 1A. U.S. Application No. 08/729,493, which issued as the '444 Patent, was filed on October 11, 1996 and claims priority as a continuation-in-part to U.S. Patent Application No. 08/550,339. The '444 Patent has 72 claims including 19 independent claims. RevoLaze became the owner of the '444 Patent by assignment. Exhibit 2A.

29. Complainants have filed a certified copy and three additional copies of the prosecution history for the '444 Patent as Appendix A. Complainants have filed four copies of each patent and technical reference identified in the prosecution history of the application from which the '444 Patent issued as Appendix B.

B. The '602 Patent – Marking of Fabrics and Other Materials Using a Laser

30. The '602 Patent, entitled “Marking of Fabrics and Other Materials Using a Laser,” was issued to Costin on October 31, 2000. A certified copy of the '602 Patent is attached to the Complaint as Exhibit 1B. U.S. Application No. 08/844,114, which issued as the '602 Patent, was filed on April 29, 1997. The '602 Patent has 154 claims including 22 independent claims. RevoLaze became the owner of the '602 Patent by assignment. Exhibit 2B.

31. Complainants have filed a certified copy and three additional copies of the prosecution history for the '602 Patent as Appendix C. Complainants have filed four copies of each patent and technical reference identified in the prosecution history of the application from which the '602 Patent issued as Appendix D.

C. The '196 Patent – Laser Method of Scribing Graphics

32. The '196 Patent, entitled "Laser Method of Scribing Graphics," was issued to Costin, et al. on June 26, 2001. A certified copy of the '196 Patent is attached to the Complaint as Exhibit 1C. U.S. Application No. 09/390,956, which issued as the '196 Patent, was filed on September 7, 1999 and claims priority as a divisional application to U.S. Patent Application No. 08/729,493, which issued as the '444 Patent. The '196 Patent has 16 claims including six independent claims. RevoLaze became the owner of the '196 Patent by assignment. Exhibit 2C.

33. Complainants have filed a certified copy and three additional copies of the prosecution history for the '196 Patent as Appendix E. Complainants have filed four copies of each patent and technical reference identified in the prosecution history of the application from which the '196 Patent issued as Appendix F.

D. The '505 Patent – Laser Processing of Materials Using Mathematical Tools

34. The '505 Patent, entitled "Laser Processing of Materials Using Mathematical Tools," was issued to Martin on December 16, 2003. A certified copy of the '505 Patent is attached to the Complaint as Exhibit 1D. U.S. Application No. 09/730,497, which issued as the '505 Patent, was filed on December 5, 2000 and claims priority to Provisional U.S. Patent Application No. 60/169,096. The '505 Patent has 115 claims including nine independent claims. RevoLaze became the owner of the '505 Patent by assignment. Exhibit 2D.

35. Complainants have filed a certified copy and three additional copies of the prosecution history for the '505 Patent as Appendix G. Complainants have filed four copies of each patent and technical reference identified in the prosecution history of the application from which the '505 Patent issued as Appendix H.

E. The '972 Patent – Material Surface Processing with a Laser that has a Scan Modulated Effective Power to Achieve Multiple Worn Looks

36. The '972 Patent, entitled “Material Surface Processing with a Laser that has a Scan Modulated Effective Power to Achieve Multiple Worn Looks,” was issued to Martin, et al. on November 16, 2004. A certified copy of the '972 Patent is attached to the Complaint as Exhibit 1E. U.S. Application No. 09/653,997, which issued as the '972 Patent, was filed on September 1, 2000 and claims priority to Provisional U.S. Patent Application No. 60/157,904. The '972 Patent has 95 claims including 12 independent claims. RevoLaze became the owner of the '972 Patent by assignment. Exhibit 2E.

37. Complainants have filed a certified copy and three additional copies of the prosecution history for the '972 Patent as Appendix I. Complainants have filed four copies of each patent and technical reference identified in the prosecution history of the application from which the '972 Patent issued as Appendix J.

F. The '815 Patent – Denim Designs from Laser Scribing

38. The '815 Patent, entitled “Denim Designs from Laser Scribing,” was issued to Costin on February 22, 2005. A certified copy of the '815 Patent is attached to the Complaint as Exhibit 1F. U.S. Application No. 10/319,163, which issued as the '815 Patent, was filed on December 14, 2002 and claims priority as a continuation of U.S. Application No. 09/408,131 and to Provisional U.S. Patent Application No. 60/102,363. The '815 Patent has 17

claims including three independent claims. RevoLaze became the owner of the '815 Patent by assignment. Exhibit 2F.

39. Complainants have filed a certified copy and three additional copies of the prosecution history for the '815 Patent as Appendix K. Complainants have filed four copies of each patent and technical reference identified in the prosecution history of the application from which the '815 Patent issued as Appendix L.

G. Foreign Counterparts

40. The Patents-in-Suit have the following foreign counterpart patents or patent applications:

- The '444 Patent – PCT Publication No. 1997/016279, Canadian Patent App. No. 2236480 (abandoned), European Patent No. 0954404 (Nationalized in Italy, Spain, France, Germany, Great Britain, and Ireland; currently undergoing opposition proceedings before the European Patent Office), Mexican Patent No. 204894 (expired), Australian Patent App. No. 19960074655 (abandoned);
- The '602 Patent – None;
- The '196 Patent – The '196 Patent is a divisional application filed from the '444 Patent. The foreign counterparts to the '196 Patent are the same as those filed from the '444 Patent;
- The '505 Patent – PCT Publication No. 2001/042554, Australian Patent App. No. 20010047119 (abandoned);
- The '972 Patent – PCT Publication No. 2001/025824, Turkish Patent No. 200201254 (issued), Chinese Patent No. 08816659.5 (issued), Mexican Patent No. 237135 (issued), Mexican Patent No. 202403 (abandoned), Australian Patent App.

No. 20000077306 (abandoned), Canadian Patent No. 2386786 (abandoned), European Patent Publication No. 1242962 (withdrawn from examination), Japanese Patent App. No. 2003511242 (abandoned), South Korean Patent No. 564715 (abandoned);

- The '815 Patent – None.

H. Licensees

41. The Asserted Patents are currently licensed to Lear Corporation; Green Bay Decking LLC; GST AutoLeather, Inc.; Nike, Inc.; DVUV, LLC; and Fins Denim Co. The Asserted Patents were previously licensed to GFSI, Inc. (Gear for Sports); Sights Denim Systems; Taylor Togs, Inc.; Final Finish Laundry, and VF Corporation, but these licenses are no longer in force.

I. Non-Technical Description of the Patented Technologies

42. For the last two decades, the denim market has demanded jeans with a worn appearance. This is achieved by abrading the denim jeans along the thighs and buttocks to give the appearance of jeans that have been worn for a long period of time. The process of choice to create this abraded or worn look had been the sandblast process, in which workers blast sand in the thigh and buttock areas to abrade the denim. In recent years, however, it has been confirmed that sandblasting denim can cause a disabling, and sometimes fatal, lung disease called silicosis for the workers.

43. Because of this deadly process, Turkey, once a predominant manufacturing country for sandblasting denim jeans, has completely banned sandblasting denim country-wide. Furthermore, all major denim apparel companies, such as Levi's, Gap, VF, and H&M, have banned the use of sandblasting in the creation of denim jeans with a worn look. The

two most acceptable alternative methods to create the worn look are hand sanding and laser abrading. This sandblasting ban has thus increased the demand for lasers to abrade denim to help satisfy the market demand for denim featuring the worn look.

44. Accordingly, denim apparel companies and their jean manufacturers are rapidly scaling up laser abrading processes to produce the denim with a worn look.

Complainants have developed laser technology to abrade denim and sought patent protection for their technology.

45. The '444 Patent is drawn to a method of scribing with a laser on material such as denim. Avoidance of undesired carbonization, melting or burn-through is achieved by controlling continuous power output, spot size of the laser beam on the material and speed of the laser relative to the material.

46. The '602 Patent is drawn to a method and apparatus for forming a design on material such as denim with a laser. Speed of the laser relative to the material is controlled between a maximum speed that will provide a perceivable change to the material and a minimum speed below which carbonization, undesired burn-through or undesired melting will occur.

47. The '196 Patent is drawn to a method to prevent over etching of material such as denim with a laser. Before the laser beam is output, the laser is set in motion relative to the material so that it is moving when the beam is output to the material.

48. The '972 Patent is drawn to a method and apparatus for changing the power of the laser beam "on the fly." A worn look on jeans has areas, for example, in the middle that appear more worn or lighter than areas on the sides or margins that appear less worn or darker. As the laser scribes the worn look it does so one line at a time (scan line), with each line above or below the next as the pattern is developed. The effective power output of the laser

changes during the course of a single scan line to provide the variation in intensity to achieve the feathering or variation in color called for by the pattern design.

49. The '505 Patent is drawn to a method of forming images on a material such as denim with a laser. The images to be formed are subdivided into picture elements called pixels. Each specific pixel has an x,y coordinate and is associated with a color or grayscale. Each grayscale is associated with a specified amount of energy from the laser to achieve the grayscale. The amount of energy that is assigned to a grayscale is determined by a mathematical operation.

50. The '815 Patent is drawn to laser scribing material such as denim. The amount of energy applied by the laser is controlled to alter the surface chemistry of a denim article without undesirably damaging the denim article. The laser thus modifies an entire width of the denim article.

IV. THE PRODUCTS AT ISSUE

A. Complainants Products

51. Complainants are innovators in laser scribing of high quality graphics and patterns on a variety of materials including denim, cotton, polyester, nylon, and silk for use in apparel and upholstery, as well as in polymer composites and natural building materials. Complainants have spent years developing and licensing the technology to partners such as Lear Corporation, a global leader in automobile seating and upholstery, Nike, Inc., Green Bay Decking, a manufacturer of composite decking, DVUV, LLC, a manufacturer of powder coated medium density fiberboard. See *infra*, Paragraphs 92 – 104 and associated Exhibits.

B. Respondent's Infringing Products

52. Respondents are each manufacturers, retailers, and/or wholesalers who make or have made and sell denim garments abraded using the Complainants' patented

technology. After investigation, Complainants have reason to believe that the Respondents' garments are abraded using a CO₂ laser, Technical Declaration of Darryl Costin ("Costin Technical Declaration"), ¶¶ 8-31 (attached as Exhibit 36A), in order to create designs on the garments or to simulate worn sections that are desirable to consumers. On information and belief, Respondents process their garments using a laser system such as that created by Jeanologia – GFK and Easy Laser. Declaration of William Murcia ("Murcia Declaration"), ¶¶ 7-11 (attached as Exhibit 37A).

V. UNLAWFUL AND UNFAIR ACTS OF THE RESPONDENTS

A. A&F

53. A&F manufactures for import, has others manufacture for import, imports into the United States, offers for sale, and/or sells in the United States after importation infringing denim garments including, but not limited to the A&F Product. The A&F Product is manufactured by a method that infringes one or more of the Asserted Claims. On information and belief, the A&F Product includes laser abrasion pores formed from a CO₂ laser using the patented method such as that used by Easy Laser and Jeanologia – GFK. Exhibit 36A, Costin Technical Declaration, ¶ 12; Exhibit 37A, Murcia Declaration, ¶¶ 7-11. On information and belief, A&F uses Easy Laser and Jeanologia – GFK technology to manufacture its products. *See* Exhibit 35A, Cynthia Martens, Jeanologia: Seeking a Friendlier Denim Finish, *Women's Wear Daily* (Nov. 9, 2011); Exhibit 35B, Jeanologia: Ultimate technology for jean finishing, *The Indian Textile Journal* (June 2012).

54. The A&F Product is made by a method infringing the Asserted Claims. Claim charts applying the Asserted Claims to the A&F Product are attached as Exhibits 8A-8F.

The claims charts demonstrate how the A&F Product meets every limitation of the Asserted Claims.

B. American Eagle Outfitters

55. AEO manufactures for import, has others manufacture for import, imports into the United States, offers for sale, and/or sells in the United States after importation infringing denim garments including, but not limited to the AEO Product. The AEO Product is manufactured by a method that infringes one or more of the Asserted Claims. On information and belief, the AEO Product includes laser abrasion pores formed from a CO₂ laser using the patented method such as that used by Easy Laser and Jeanologia – GFK. Exhibit 36A, Costin Technical Declaration, ¶ 13; Exhibit 37A, Murcia Declaration, ¶¶ 7-11. On information and belief, AEO uses Easy Laser and Jeanologia – GFK lasers and methods to create the AEO Product. *See* Exhibit 35C, Easy Laser, Our Customers.

56. The AEO Product is made by a method infringing the Asserted Claims. Claim charts applying the Asserted Claims to the AEO Product are attached as Exhibits 9A-9F. The claims charts demonstrate how the AEO Product meets every limitation of the Asserted Claims.

C. BlankNYC

57. BlankNYC manufactures for import, has others manufacture for import, imports into the United States, offers for sale, and/or sells in the United States after importation infringing denim garments including, but not limited to the BlankNYC Product. The BlankNYC Product is manufactured by a method that infringes one or more of the Asserted Claims. On information and belief, the BlankNYC Product includes laser abrasion pores formed from a CO₂

laser using the patented method such as that used by Easy Laser and Jeanologia – GFK. Exhibit 36A, Costin Technical Declaration, ¶ 14; Exhibit 37A, Murcia Declaration, ¶¶ 7-11.

58. The BlankNYC Product is made by a method infringing the Asserted Claims. Claim charts applying the Asserted Claims to the BlankNYC Product are attached as Exhibits 10A-10F. The claims charts demonstrate how the BlankNYC Product meets every limitation of the Asserted Claims.

D. Buckle

59. Buckle manufactures for import, has others manufacture for import, imports into the United States, offers for sale, and/or sells in the United States after importation infringing denim garments including, but not limited to the Buckle Product. The Buckle Product is manufactured by a method that infringes one or more of the Asserted Claims. On information and belief, the Buckle Product includes laser abrasion pores formed from a CO₂ laser using the patented method such as that used by Easy Laser and Jeanologia – GFK. Exhibit 36A, Costin Technical Declaration, ¶ 15; Exhibit 37A, Murcia Declaration, ¶¶ 7-11. On information and belief, Buckle uses Easy Laser and Jeanologia – GFK lasers and methods to create the Buckle Product. *See* Exhibit 35D, Jeanologia dominates Mexican garment finishing market, fibre 2 fashion (Mar. 11, 2014).

60. The Buckle Product is made by a method infringing the Asserted Claims. Claim charts applying the Asserted Claims to the Buckle Product are attached as Exhibits 11A-11F. The claims charts demonstrate how the Buckle Product meets every limitation of the Asserted Claims.

E. **Buffalo**

61. Buffalo manufactures for import, has others manufacture for import, imports into the United States, offers for sale, and/or sells in the United States after importation infringing denim garments including, but not limited to the Buffalo Product. The Buffalo Product is manufactured by a method that infringes one or more of the Asserted Claims. On information and belief, the Buffalo Product includes laser abrasion pores formed from a CO₂ laser using the patented method such as that used by Easy Laser and Jeanologia – GFK. Exhibit 36A, Costin Technical Declaration, ¶ 16; Exhibit 37A, Murcia Declaration, ¶¶ 7-11.

62. The Buffalo Product is made by a method infringing the Asserted Claims. Claim charts applying the Asserted Claims to the Buffalo Product are attached as Exhibits 12A-12F. The claims charts demonstrate how the Buffalo Product meets every limitation of the Asserted Claims.

F. **[Reserved]**

63. [Reserved].

64. [Reserved].

G. **Diesel**

65. Diesel manufactures for import, has others manufacture for import, imports into the United States, offers for sale, and/or sells in the United States after importation infringing denim garments including, but not limited to the Diesel Product. The Diesel Product is manufactured by a method that infringes one or more of the Asserted Claims. On information and belief, the Diesel Product includes laser abrasion pores formed from a CO₂ laser using the patented method such as that used by Easy Laser and Jeanologia – GFK. Exhibit 36A, Costin Technical Declaration, ¶ 18; Exhibit 37A, Murcia Declaration, ¶¶ 7-11. On information and

belief, Diesel uses Easy Laser and Jeanologia – GFK lasers and methods to create the Diesel Product. *See* Exhibit 35C, Easy Laser, Our Customers.

66. The Diesel Product is made by a method infringing the Asserted Claims. Claim charts applying the Asserted Claims to the Diesel Product are attached as Exhibits 14A-14F. The claims charts demonstrate how the Diesel Product meets every limitation of the Asserted Claims.

H. DL1961

67. DL1961 manufactures for import, has others manufacture for import, imports into the United States, offers for sale, and/or sells in the United States after importation infringing denim garments including, but not limited to the DL1961 Product. The DL1961 Product is manufactured by a method that infringes one or more of the Asserted Claims. On information and belief, the DL1961 Product includes laser abrasion pores formed from a CO₂ laser using the patented method such as that used by Easy Laser and Jeanologia – GFK. Exhibit 36A, Costin Technical Declaration, ¶ 19; Exhibit 37A, Murcia Declaration, ¶¶ 7-11. DL1961 admits that it uses Jeanologia – GFK equipment in the production of its jeans. Exhibit 35F, Panel: Industry Drives Sustainability Effort, Women’s Wear Daily at 8 (July 24, 2013) (“DL1961 has employed both Lenzing fibers and, in its parent company’s plant in Pakistan, Jeanologia’s equipment.”).

68. The DL1961 Product is made by a method infringing the Asserted Claims. Claim charts applying the Asserted Claims to the DL1961 Product are attached as Exhibits 15A-15F. The claims charts demonstrate how the DL1961 Product meets every limitation of the Asserted Claims.

I. **Eddie Bauer**

69. Eddie Bauer manufactures for import, has others manufacture for import, imports into the United States, offers for sale, and/or sells in the United States after importation infringing denim garments including, but not limited to the Eddie Bauer Product. The Eddie Bauer Product is manufactured by a method that infringes one or more of the Asserted Claims. On information and belief, the Eddie Bauer Product includes laser abrasion pores formed from a CO₂ laser using the patented method such as that used by Easy Laser and Jeanologia – GFK. Exhibit 36A, Costin Technical Declaration, ¶ 20; Exhibit 37A, Murcia Declaration, ¶¶ 7-11.

70. The Eddie Bauer Product is made by a method infringing the Asserted Claims. Claim charts applying the Asserted Claims to the Eddie Bauer Product are attached as Exhibits 16A-16F. The claims charts demonstrate how the Eddie Bauer Product meets every limitation of the Asserted Claims.

J. **Gap**

71. Gap manufactures for import, has others manufacture for import, imports into the United States, offers for sale, and/or sells in the United States after importation infringing denim garments including, but not limited to the Gap Product. The Gap Product is manufactured by a method that infringes one or more of the Asserted Claims. On information and belief, the Gap Product includes laser abrasion pores formed from a CO₂ laser using the patented method such as that used by Easy Laser and Jeanologia – GFK. Exhibit 36A, Costin Technical Declaration, ¶ 21; Exhibit 37A, Murcia Declaration, ¶¶ 7-11. On information and belief, Gap uses Easy Laser and Jeanologia – GFK lasers and methods to create the Gap Product. *See* Exhibit 35B, Jeanologia: Ultimate technology for jean finishing, The Indian Textile Journal (June 2012); Exhibit 35C, Easy Laser, Our Customers.

72. The Gap Product is made by a method infringing the Asserted Claims.

Claim charts applying the Asserted Claims to the Gap Product are attached as Exhibits 17A-17F.

The claims charts demonstrate how the Gap Product meets every limitation of the Asserted Claims.

K. Guess?

73. Guess? manufactures for import, has others manufacture for import, imports into the United States, offers for sale, and/or sells in the United States after importation infringing denim garments including, but not limited to the Guess? Product. The Guess? Product is manufactured by a method that infringes one or more of the Asserted Claims. On information and belief, the Guess? Product includes laser abrasion pores formed from a CO₂ laser using the patented method such as that used by Easy Laser and Jeanologia – GFK. Exhibit 36A, Costin Technical Declaration, ¶ 22; Exhibit 37A, Murcia Declaration, ¶¶ 7-11. On information and belief, Guess? uses Easy Laser and Jeanologia – GFK lasers and methods to create the Guess? Product. *See* Exhibit 35D, Jeanologia dominates Mexican garment finishing market, fibre 2 fashion (Mar. 11, 2014).

74. The Guess? Product is made by a method infringing the Asserted Claims.

Claim charts applying the Asserted Claims to the Guess? Product are attached as Exhibits 18A-

18F. The claims charts demonstrate how the Guess? Product meets every limitation of the Asserted Claims.

L. H&M

75. H&M manufactures for import, has others manufacture for import, imports into the United States, offers for sale, and/or sells in the United States after importation infringing denim garments including, but not limited to the H&M Product. The H&M Product is

manufactured by a method that infringes one or more of the Asserted Claims. On information and belief, the H&M Product includes laser abrasion pores formed from a CO₂ laser using the patented method such as that used by Easy Laser and Jeanologia – GFK. Exhibit 36A, Costin Technical Declaration, ¶ 23; Exhibit 37A, Murcia Declaration, ¶¶ 7-11. On information and belief, H&M uses Easy Laser and Jeanologia – GFK technology to manufacture the H&M Product. *See* Exhibit 35A, Cynthia Martens, Jeanologia: Seeking a Friendlier Denim Finish, *Women’s Wear Daily* (Nov. 9, 2011).

76. The H&M Product is made by a method infringing the Asserted Claims. Claim charts applying the Asserted Claims to the H&M Product are attached as Exhibits 19A-19F. The claims charts demonstrate how the H&M Product meets every limitation of the Asserted Claims.

M. Just Cavalli

77. Just Cavalli manufactures for import, has others manufacture for import, imports into the United States, offers for sale, and/or sells in the United States after importation infringing denim garments including, but not limited to the Just Cavalli Product. The Just Cavalli Product is manufactured by a method that infringes one or more of the Asserted Claims. On information and belief, the Just Cavalli Product includes laser abrasion pores formed from a CO₂ laser using the patented method such as that used by Easy Laser and Jeanologia – GFK. Exhibit 36A, Costin Technical Declaration, ¶ 24; Exhibit 37A, Murcia Declaration, ¶¶ 7-11.

78. The Just Cavalli Product is made by a method infringing the Asserted Claims. Claim charts applying the Asserted Claims to the Just Cavalli Product are attached as Exhibits 20A-20F. The claims charts demonstrate how the Just Cavalli Product meets every limitation of the Asserted Claims.

N. **Koos**

79. Koos manufactures for import, has others manufacture for import, imports into the United States, offers for sale, and/or sells in the United States after importation infringing denim garments including, but not limited to the Koos Products. The Koos Products are manufactured by a method that infringes one or more of the Asserted Claims. On information and belief, the Koos Products include laser abrasion pores formed from a CO₂ laser using the patented method such as that used by Easy Laser and Jeanologia – GFK. Exhibit 36A, Costin Technical Declaration, ¶¶ 25-26; Exhibit 37A, Murcia Declaration, ¶¶ 7-11. On information and belief, Koos uses Easy Laser and Jeanologia – GFK lasers and methods to create the Koos Products. *See* Exhibit 35D, Jeanologia dominates Mexican garment finishing market, fibre 2 fashion (Mar. 11, 2014). In addition, Koos has purchased Jeanologia equipment. Exhibit 35G, Ocean Bill of Lading for Koos (showing importation of Jeanologia equipment by Koos Manufacturing). On information and belief, Koos uses the Jeanologia equipment to manufacture the Koos Products.

80. The Koos Products are made by a method infringing the Asserted Claims. Claim charts applying the Asserted Claims to the Koos Products are attached as Exhibits 21A-21F and 22A-22F. The claims charts demonstrate how the Koos Products meet every limitation of the Asserted Claims.

O. **Levi's**

81. Levi's manufactures for import, has others manufacture for import, imports into the United States, offers for sale, and/or sells in the United States after importation infringing denim garments including, but not limited to the Levi's Product. The Levi's Product is manufactured by a method that infringes one or more of the Asserted Claims. On information

and belief, the Levi's Product includes laser abrasion pores formed from a CO₂ laser using the patented method such as that used by Easy Laser and Jeanologia – GFK. Exhibit 36A, Costin Technical Declaration, ¶ 27; Exhibit 37A, Murcia Declaration, ¶¶ 7-11. On information and belief, Levi's uses Easy Laser and Jeanologia – GFK lasers and methods to create the Levi's Product. *See* Exhibit 35C, Easy Laser, Our Customers. Levi's also provides instructions to its employees on a laser etching process "involv[ing] the use of lasers to fade dyes, giving garments a worn and abraded appearance. This technique may also be used to create faded images or letters." Exhibit 35H, Environment, Health and Safety Handbook, Levi Strauss & Co. at 87 (v2.0 April 2007).

82. The Levi's Product is made by a method infringing the Asserted Claims. Claim charts applying the Asserted Claims to the Levi's Product are attached as Exhibits 23A-23F. The claims charts demonstrate how the Levi's Product meets every limitation of the Asserted Claims.

P. Lucky

83. Lucky manufactures for import, has others manufacture for import, imports into the United States, offers for sale, and/or sells in the United States after importation infringing denim garments including, but not limited to the Lucky Product. The Lucky Product is manufactured by a method that infringes one or more of the Asserted Claims. On information and belief, the Lucky Product includes laser abrasion pores formed from a CO₂ laser using the patented method such as that used by Easy Laser and Jeanologia – GFK. Exhibit 36A, Costin Technical Declaration, ¶ 28; Exhibit 37A, Murcia Declaration, ¶¶ 7-11. On information and belief, Lucky uses Easy Laser and Jeanologia – GFK lasers and methods to create the Lucky

Product. *See* Exhibit 35D, Jeanologia dominates Mexican garment finishing market, fibre 2 fashion (Mar. 11, 2014).

84. The Lucky Product is made by a method infringing the Asserted Claims. Claim charts applying the Asserted Claims to the Lucky Product are attached as Exhibits 24A-24F. The claims charts demonstrate how the Lucky Product meets every limitation of the Asserted Claims.

Q. Replay

85. Replay manufactures for import, has others manufacture for import, imports into the United States, offers for sale, and/or sells in the United States after importation infringing denim garments including, but not limited to the Replay Product. The Replay Product is manufactured by a method that infringes one or more of the Asserted Claims. Replay admits that it manufactures, has manufactured, and/or distributes these products using laser-abrading technology. Exhibit 7H, Replay Laserblast – Official Teaser Video *available at* <https://www.youtube.com/watch?v=csHda3aEqIk&index=7&list=PLFFE50865E37B4517>. On information and belief, Replay uses Easy Laser and Jeanologia – GFK lasers and methods to create the Replay Product. *Id.* On information and belief, the Replay Product includes laser abrasion pores formed from a CO₂ laser using the patented method such as that used by Easy Laser and Jeanologia – GFK. Exhibit 36A, Costin Technical Declaration, ¶ 29; Exhibit 37A, Murcia Declaration, ¶¶ 7-11.

86. The Replay Product is made by a method infringing the Asserted Claims. Claim charts applying the Asserted Claims to the Replay Product are attached as Exhibits 25A-25F. The claims charts demonstrate how the Replay Product meets every limitation of the Asserted Claims.

R. **VF Corp.**

87. VF manufactures for import, has others manufacture for import, imports into the United States, offers for sale, and/or sells in the United States after importation infringing denim garments including, but not limited to the VF Product. The VF Product is manufactured by a method that infringes one or more of the Asserted Claims. On information and belief, the VF Product includes laser abrasion pores formed from a CO₂ laser using the patented method such as that used by Easy Laser and Jeanologia – GFK. Exhibit 36A, Costin Technical Declaration, ¶ 30; Exhibit 37A, Murcia Declaration, ¶¶ 7-11. On information and belief, VF uses Easy Laser and Jeanologia – GFK lasers and methods to create the VF Product. *See* Exhibit 35D, Jeanologia dominates Mexican garment finishing market, fibre 2 fashion (Mar. 11, 2014).

88. The VF Product is made by a method infringing the Asserted Claims. Claim charts applying the Asserted Claims to the VF Product are attached as Exhibits 26A-26F. The claims charts demonstrate how the VF Product meets every limitation of the Asserted Claims.

VI. SPECIFIC INSTANCES OF IMPORTATION AND SALE

89. Each Accused Product is marked as having been made outside of the United States and was sold in the United States after importation or sold for importation into the United States. Exhibit 6A, Ripley Declaration ¶¶ 4-58. The A&F Product was manufactured in Guatemala. *Id.* ¶ 6. The Koos Products, AEO Product, Buckle Product, Guess? Product, Levi's Product, Lucky Product, and VF Product were manufactured in Mexico. *Id.* ¶¶ 9, 15, 36, 49, 52, and 58. The BlankNYC Product and Gap Product were manufactured in China. *Id.* ¶ 12 and 33. The Buffalo Product was manufactured in Thailand. *Id.* ¶ 18. The Diesel Product was manufactured in Italy. *Id.* ¶ 24. The DL1961 Product was manufactured in Pakistan. *Id.* ¶ 27.

The Eddie Bauer Product was manufactured in Sri Lanka. *Id.* ¶ 30. The H&M Product was manufactured in Turkey. *Id.* ¶ 39. The Just Cavalli Product was manufactured in Romania. *Id.* ¶ 42. The Replay Product was manufactured in Tunisia. *Id.* ¶ 55.

VII. CLASSIFICATION OF THE INFRINGING PRODUCTS UNDER THE HARMONIZED TARIFF SCHEDULE OF THE UNITED STATES.

90. The Accused Products are believed to fall within at least the following classifications of the harmonized tariff schedules of the United States: 6203.42.4011 and 6204.62.4011. These classifications are intended for illustrative purposes only and are not intended to restrict the scope or type of product accused of infringing the Asserted Patents.

VIII. RELATED LITIGATION

91. Complainant RevoLaze has filed complaints alleging patent infringement in the U.S. District Court for the Northern District of Ohio on August 15, 2014, styled as RevoLaze, LLC, v. Abercrombie & Fitch Co. (Case No. 1:14-cv-01797-PAG), RevoLaze, LLC, v. American Eagle Outfitters, Inc. (Case No. 1:14-cv-01799-PAG), RevoLaze, LLC, v. BBC Apparel Group, LLC, et al. (Case No. 1:14-cv-01800-DCN), RevoLaze, LLC, v. The Buckle, Inc. (Case No. 1:14-cv-01801-PAG), RevoLaze, LLC, v. Buffalo International ULC, et al. (Case No. 1:14-cv-01803-JG), RevoLaze, LLC, v. Diesel S.p.A. (Case No. 1:14-cv-01806-DAP), RevoLaze, LLC, v. DL1961 Premium Denim Inc. (Case No. 1:14-cv-01807-DCN), RevoLaze, LLC, v. Eddie Bauer LLC (Case No. 1:14-cv-01809-DCN), RevoLaze, LLC, v. The Gap, Inc. (Case No. 1:14-cv-01821), RevoLaze, LLC, v. Guess?, Inc. (Case No. 1:14-cv-01818), RevoLaze, LLC, v. H&M Hennes & Mauritz AB, et al. (Case No. 1:14-cv-01812-PAG), RevoLaze, LLC, v. Roberto Cavalli S.p.A. (Case No. 1:14-cv-01819), RevoLaze, LLC, v. Koos Manufacturing, Inc. (Case No. 1:14-cv-01814), RevoLaze, LLC, v. Levi Strauss & Co. (Case No. 1:14-cv-01816), RevoLaze, LLC, v. Lucky Brand Dungarees, Inc. (Case No. 1:14-cv-01817),

RevoLaze, LLC, v. Fashion Box S.p.A. (Case No. 1:14-cv-01815), and RevoLaze, LLC, v. VF Corporation (Case No. 1:14-cv-01820), accusing each Respondent of infringing one or more of the Asserted Patents.

IX. **DOMESTIC INDUSTRY**

92. A domestic industry exists and is in the process of being established within the United States as defined by 19 U.S.C. §§1337(a)(3)(A)-(C) relating to significant investments in plant and equipment, significant employment of labor and capital, and significant investment in the exploitation of the Asserted Patents, including engineering and development of domestic industry products. The identified domestic industry products covered by one or more Asserted Claim include the domestic industry of Complainants and their licensees.

A. **Technical Prong**

93. RevoLaze is currently in the process of establishing a domestic industry by utilizing linear processing of rolls of denim or other materials using at least one embodiment of the invention as claimed in the '444 Patent, the '602 Patent, the '196 Patent, the '505 Patent, the '972 Patent, and the '815 Patent. Complainants have attached claim charts detailing how the linear processing industry practices the Asserted Patents. Exhibits 27A-27F.

94. Complainants are currently in the process of developing a domestic industry for sports apparel marking. By this industry, consumers will be able to purchase apparel having their favorite sports team's logo, likeness, name, or other mark laser etched into an item of apparel. The sports apparel marking process utilizes at least one embodiment of the invention as claimed in the '444 Patent, the '602 Patent, the '196 Patent, the '505 Patent, the '972 Patent, and the '815 Patent. Complainants have attached claim charts detailing how the sports apparel industry practices the Asserted Patents. Exhibits 28A-28F.

95. Complainants have licensed the claimed technology to Green Bay Decking LLC to scribe simulated wood grain patterns on composite decking to make it appear more realistic like natural wood decking. Exhibit 4D, Green Bay Decking LLC License. The decking industry utilizes at least one embodiment of the invention as claimed in the '444 Patent, the '602 Patent, the '196 Patent, the '505 Patent, the '972 Patent, and the '815 Patent. Complainants have attached claim charts detailing how the composite decking material industry practices the Asserted Patents. Exhibits 29A-29F.

96. Complainants have licensed the claimed technology to Lear Corporation to scribe graphics and patterns on automotive products. Exhibit 4C, Lear Corp. License. Lear's use of the patented technology for automotive cloth interiors utilizes at least one embodiment of the invention as claimed in the '444 Patent, the '602 Patent, the '196 Patent, the '505 Patent, the '972 Patent, and the '815 Patent. Complainants have attached claim charts detailing how Lear's automotive upholstery industry practices the Asserted Patents. Exhibits 30A-30F.

97. Complainants have licensed the claimed technology to GST AutoLeather, Inc. to scribe graphics and patterns on leather upholstery products. Exhibit 4B, GST AutoLeather, Inc. License. GST's use of the patented technology for leather upholstery utilizes at least one embodiment of the invention as claimed in the '444 Patent, the '602 Patent, the '196 Patent, and the '505 Patent. Complainants have attached claim charts detailing how GST's leather upholstery industry practices the Asserted Patents. Exhibits 31A-31D.

98. Complainants have licensed the claimed technology to DVUV, LLC to scribe graphic and patterns on medium density fiberboard. Exhibit 4A, DVUV, LLC License. The laser etched medium density fiberboard industry utilizes at least one embodiment of the invention as claimed in the '444 Patent, the '602 Patent, the '196 Patent, the '505 Patent, and

the '815 Patent. Complainants have attached claim charts detailing how DVUV's fiberboard industry practices the Asserted Patents. Exhibits 32A-32E.

99. RevoLaze is currently in the process of developing a domestic industry by utilizing high-speed laser abrasion of denim jeans using at least one embodiment of the invention as claimed in the '444 Patent, the '602 Patent, the '196 Patent, the '505 Patent, the '972 Patent, and the '815 Patent. Complainants have attached claim charts detailing how the high-speed abrasion industry practices the Asserted Patents. Exhibits 33A-33F.

B. Economic Prong

100. Both Complainants and their licensees have made in the past and are continuing to make substantial investments in plants and equipment, labor and capital, and exploitation of the Asserted Patents and products manufactured utilizing the methods and systems claimed in the Asserted Patents. *See* Exhibit 34A, Domestic Industry Declaration of Darryl J. Costin, Ph.D. ("Costin Domestic Industry Declaration") and associated Exhibits.

101. Specifically, RevoLaze has made significant investments to operate offices, research and development, and manufacturing facilities in Westlake, Ohio and St. Paul, Minnesota. In the Westlake, Ohio facility, Complainants operate approximately

of office space and of research and development space. Exhibit 34A, Costin Domestic Industry Declaration, ¶ 10. In the St. Paul facility, Complainants operate approximately of manufacturing and research and development space in conjunction with LasX Industries. Exhibit 34A, Costin Domestic Industry Declaration, ¶ 12-13. RevoLaze is in the process of opening a linear processing system at its Westlake facility for which approximately has been contracted for the development and initial operation of the linear processing system. Exhibit 34A, Costin Domestic Industry Declaration, ¶ 16. Over

the past five years, Complainants have also invested approximately [REDACTED] for other laser equipment, manufacturing and office space, maintenance and repairs, and equipment rental. Exhibit 34A, Costin Domestic Industry Declaration, ¶ 22.

102. RevoLaze, TechnoLines, their affiliates, and their licensees have invested significant resources in labor and capital as well. Between 2010 and 2014, they invested approximately [REDACTED] for the research, development, and commercialization of the patented technology including the various products identified in Exhibits 29A-29F, 30A-30F, 31A-31D, 32A-32E, and 33A-33F. Exhibit 34A, Costin Domestic Industry Declaration, ¶ 30-130. In addition, personnel costs between 2010 and May 31, 2014 have totaled approximately [REDACTED] for Complainants. Exhibit 34A, Costin Domestic Industry Declaration, ¶ 29.

103. Complainants have worked to exploit the claimed technology continuously since the Asserted Patents were filed. Complainants have participated in numerous trade shows showcasing the patented technology at a cost of approximately [REDACTED] over the past two years. Exhibit 34A, Costin Domestic Industry Declaration, ¶¶ 36-63. Complainants have also licensed the Asserted Patents and Complainants' technical know-how to multiple licensees over the course of the last several years, and are continuing to explore new market potential and partners. Exhibit 34A, Costin Domestic Industry Declaration ¶¶ 64-130.

104. Complainants have developed hundreds of graphic files for laser etching for numerous customers, including one or more of the Respondents, throughout Complainants history in response to sample requests. Exhibit 34A, Costin Domestic Industry Declaration ¶¶ 119-130.

X. GENERAL EXCLUSION ORDER

105. There is a pattern of violation of the 19 U.S.C. § 1337, as evidenced by the large number of respondents, and it is difficult to identify all sources of infringing products.

Many manufacturing facilities in many different countries manufacture infringing garments for apparel companies, including the Respondents. It is difficult for Complainants to identify all apparel companies whose apparel is manufactured by the infringing processes. Likewise, it is difficult for Complainants to identify all manufacturing facilities that apparel companies use to manufacture infringing garments. Accordingly, Complainants request a general exclusion order be entered by the United States International Trade Commission.

XI. RELIEF REQUESTED

106. Complainants respectfully request that the United States International Trade Commission:

a) institute an immediate investigation pursuant to Section 337(b)(1) of the Tariff Act of 1930 (19 U.S.C. § 1337(b)(1)) into the violations by Respondents of Section 337 arising from the unlawful importation into the United States, sale for importation, and/or sale within the United States after importation of Respondents denim garments that are made and/or processed by methods that infringe the Asserted Claims of the Asserted Patents.

b) schedule and conduct a hearing pursuant to Section 337(c) for purposes of receiving evidence and hearing argument whether there has been a violation of Section 337, and, following the hearing, determine that there has been a violation of Section 337;

c) issue a permanent general exclusion order pursuant to 19 U.S.C. § 1337(d)(2)(B) forbidding entry into the United States of all denim garments manufactured or processed by methods that infringe the Asserted Patents ; or, in the alternative;

d) issue a limited exclusion order pursuant to 19 U.S.C. §1337(d)(1) forbidding entry of denim garments imported, sold for importation, or sold in the United State following importation by Respondents that infringe the Asserted Patents;

e) issue permanent cease-and-desist orders pursuant to 19 U.S.C. §1337(f) directing Respondents to cease and desist from the importation, sale, offer for sale, advertising, or solicitation for sale by Respondents of denim garments that are manufactured or processed by methods that infringe one or more of the Asserted Patents;

f) grant such other relief as the Commission deems just and proper based on the facts determined by the investigation.

Dated: August 18, 2014

Respectfully submitted,



Mark L. Hogge
Shailendra K. Maheshwari
Steven J. Stein
Nicholas H. Jackson
DENTONS US LLP
1301 K Street, N.W.
6th Floor, East Tower
Washington, D.C. 20005

September 17, 2014
News Release 14-094
Inv. No. 337-TA-930
Contact: Peg O'Laughlin, 202-205-1819

**USITC INSTITUTES SECTION 337 INVESTIGATION OF CERTAIN LASER
ABRADED DENIM GARMENTS**

The U.S. International Trade Commission (USITC) has voted to institute an investigation of certain laser abraded denim garments. The products at issue in this investigation are denim garments, including jeans and leggings, that have been abraded with a laser to apply designs or to simulate wear.

The investigation is based on a complaint filed by RevoLaze, LLC, and TechnoLines, LLC, both of Westlake, OH, on August 18, 2014. The complaint alleges violations of section 337 of the Tariff Act of 1930 in the importation into the United States and sale of certain laser abraded denim garments that infringe patents asserted by the complainants. The complainants request that the USITC issue a general exclusion order, or in the alternative a limited exclusion order, and cease and desist orders.

The USITC has identified the following as respondents in this investigation:

Abercrombie & Fitch Co. of New Albany, OH;
American Eagle Outfitters, Inc., of Pittsburgh, PA;
BBC Apparel Group, LLC, of New York, NY;
Gotham Licensing Group, LLC, of New York, NY;
The Buckle, Inc., of Kearney, NE;
Buffalo International ULC of Montreal, Quebec, Canada;
1724982 Alberta ULC of Montreal, Quebec, Canada;
Diesel S.p.A. of Breganze (VI), Italy;
DL1961 Premium Denim Inc. of New York, NY;
Eddie Bauer LLC of Bellevue, WA;
The Gap, Inc., of San Francisco, CA;
Guess?, Inc., of Los Angeles, CA;
H&M Hennes & Mauritz AB of Stockholm, Sweden;
H&M Hennes & Mauritz LP of New York, NY;
Roberto Cavalli S.p.A. of Milan, Italy;
Koos Manufacturing, Inc., of South Gate, CA;
Levi Strauss & Co. of San Francisco, CA;
Lucky Brand Dungarees, Inc., of Los Angeles, CA;
Fashion Box S.p.A. of Asolo (Treviso), Italy; and
VF Corporation of Greensboro, NC.

By instituting this investigation (337-TA-930), the USITC has not yet made any decision on the merits of the case. The USITC's Chief Administrative Law Judge will assign the case to one of the USITC's administrative law judges (ALJ), who will schedule and hold an evidentiary

hearing. The ALJ will make an initial determination as to whether there is a violation of section 337; that initial determination is subject to review by the Commission.

The USITC will make a final determination in the investigation at the earliest practicable time. Within 45 days after institution of the investigation, the USITC will set a target date for completing the investigation. USITC remedial orders in section 337 cases are effective when issued and become final 60 days after issuance unless disapproved for policy reasons by the U.S. Trade Representative within that 60-day period.

#

Levi's Settles ITC Patent Infringement Case

 rivetandjeans.com/levis-settles-itc-patent-infringement-case/

Levi Strauss & Co. has settled a denim technology infringement case through the U.S. International Trade Commission (ITC). The company agreed to enter into a licensing agreement with RevoLaze, LLC and TechnoLines, LLC, which filed a complaint last August claiming infringement on six patents regarding laser abraded denim garments.

RevoLaze said it holds 29 patents for laser inscribing methods that apply patterns and worn-in looks to various materials, including denim. The laser abrasion technology is used as an alternative to sandblasting techniques, which can be harmful to workers' health.

According to the family-operated company, RevoLaze CEO Darryl Costin, PhD., has spent 20 years developing high-speed, high-power laser scribing technology for the denim industry.

"We have worked very hard over the last two decades to invent and patent our proprietary laser scribing technology to benefit the denim industry," Costin said. "Our goal has always been to do the right thing. We want to help protect workers. We want to conserve the environment and significantly contribute to the denim industry's green movement. We want the denim industry to continue growing and to realize cost, quality, throughput and environmental advantages with RevoLaze technology."

Levi's was one of 17 companies the ITC complaint targeted, including VF Corp, Hennes & Mauritz and Gap Inc. BBC Apparel, Eddie Bauer, Fashion Box SpA and Gotham Licensing Group and have already settled the cases against them.



(19) **United States**

(12) **Patent Application Publication**
Poupyrev

(10) **Pub. No.: US 2016/0282988 A1**

(43) **Pub. Date: Sep. 29, 2016**

(54) **TWO-LAYER INTERACTIVE TEXTILES**
(71) Applicant: **Google Inc.**, Mountain View, CA (US)
(72) Inventor: **Ivan Poupyrev**, Sunnyvale, CA (US)
(21) Appl. No.: **14/959,730**
(22) Filed: **Dec. 4, 2015**

(52) **U.S. Cl.**
CPC **G06F 3/044** (2013.01); **G06F 3/0416**
(2013.01); **D03D 25/005** (2013.01); **D03D**
1/0088 (2013.01); **G06F 2203/04102** (2013.01);
G06F 2203/04111 (2013.01); **D03D 2700/0166**
(2013.01); **D10B 2401/16** (2013.01); **D10B**
2401/18 (2013.01); **G06F 2203/04103**
(2013.01)

Related U.S. Application Data

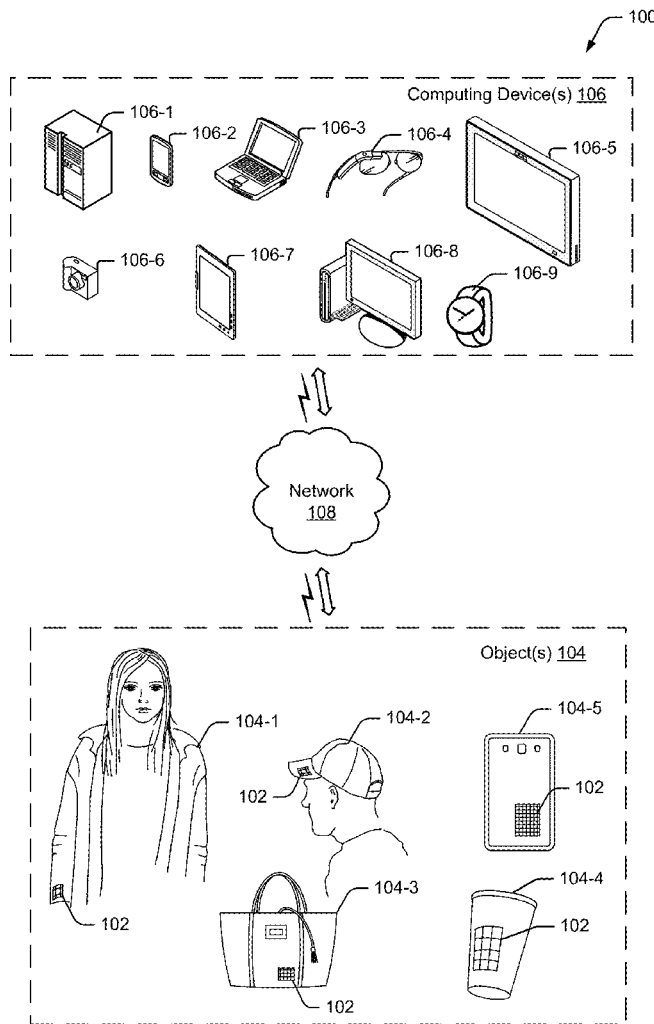
(60) Provisional application No. 62/138,831, filed on Mar. 26, 2015.

Publication Classification

(51) **Int. Cl.**
G06F 3/044 (2006.01)
D03D 25/00 (2006.01)
D03D 1/00 (2006.01)
G06F 3/041 (2006.01)

(57) **ABSTRACT**

This document describes two-layer interactive textiles. In one or more implementations, the interactive textile includes a top textile layer and a bottom textile layer. Conductive threads are woven into the top textile layer and the bottom textile layer. When the top textile layer is combined with the bottom textile layer, the conductive threads from each layer form a capacitive touch sensor that is configured to detect touch-input. The bottom textile layer is not visible and couples the capacitive through sensor to electronic components, such as a controller, a wireless interface, an output device (e.g., an LED, a display, or speaker), and so forth.



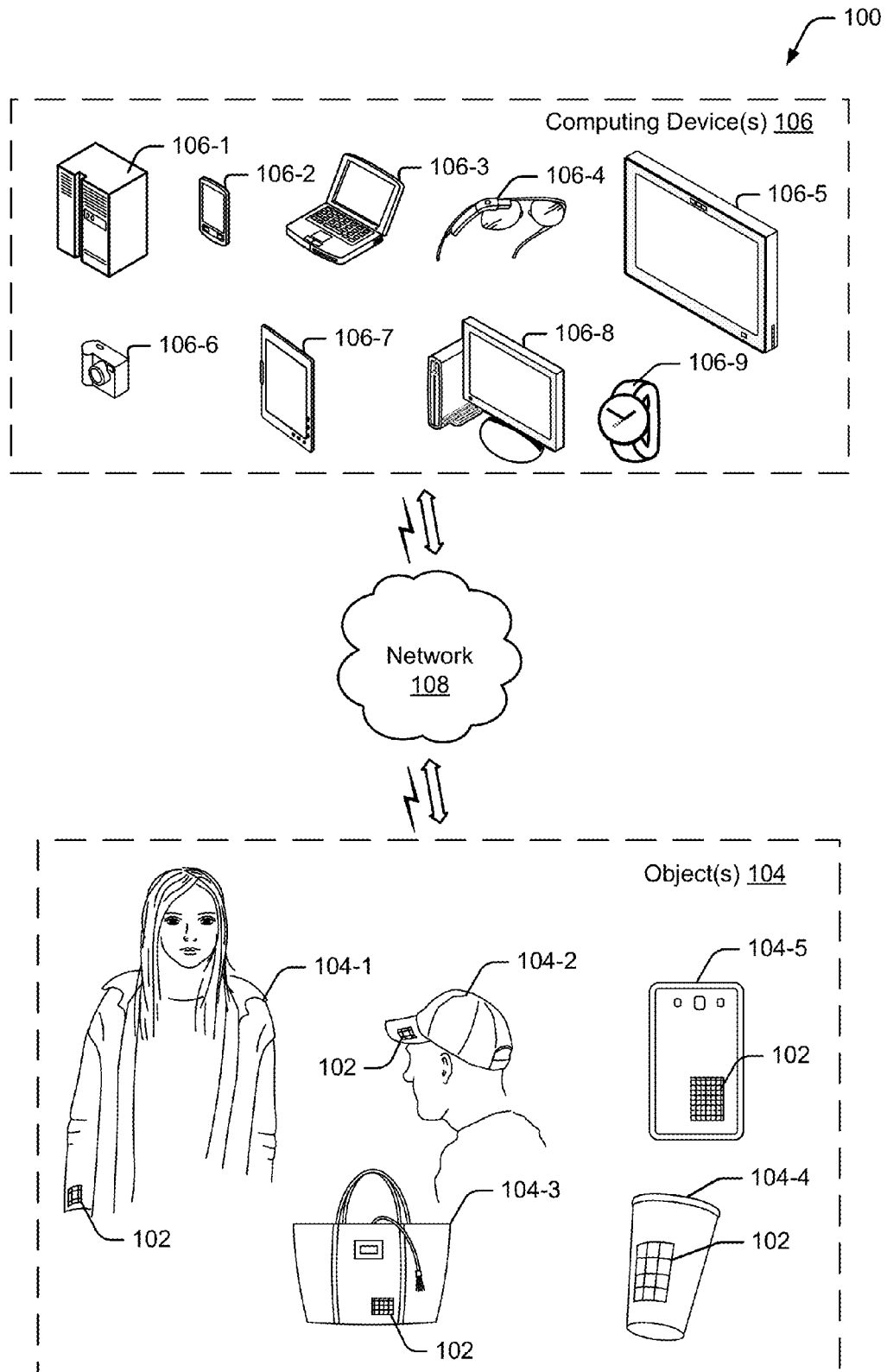


Fig. 1

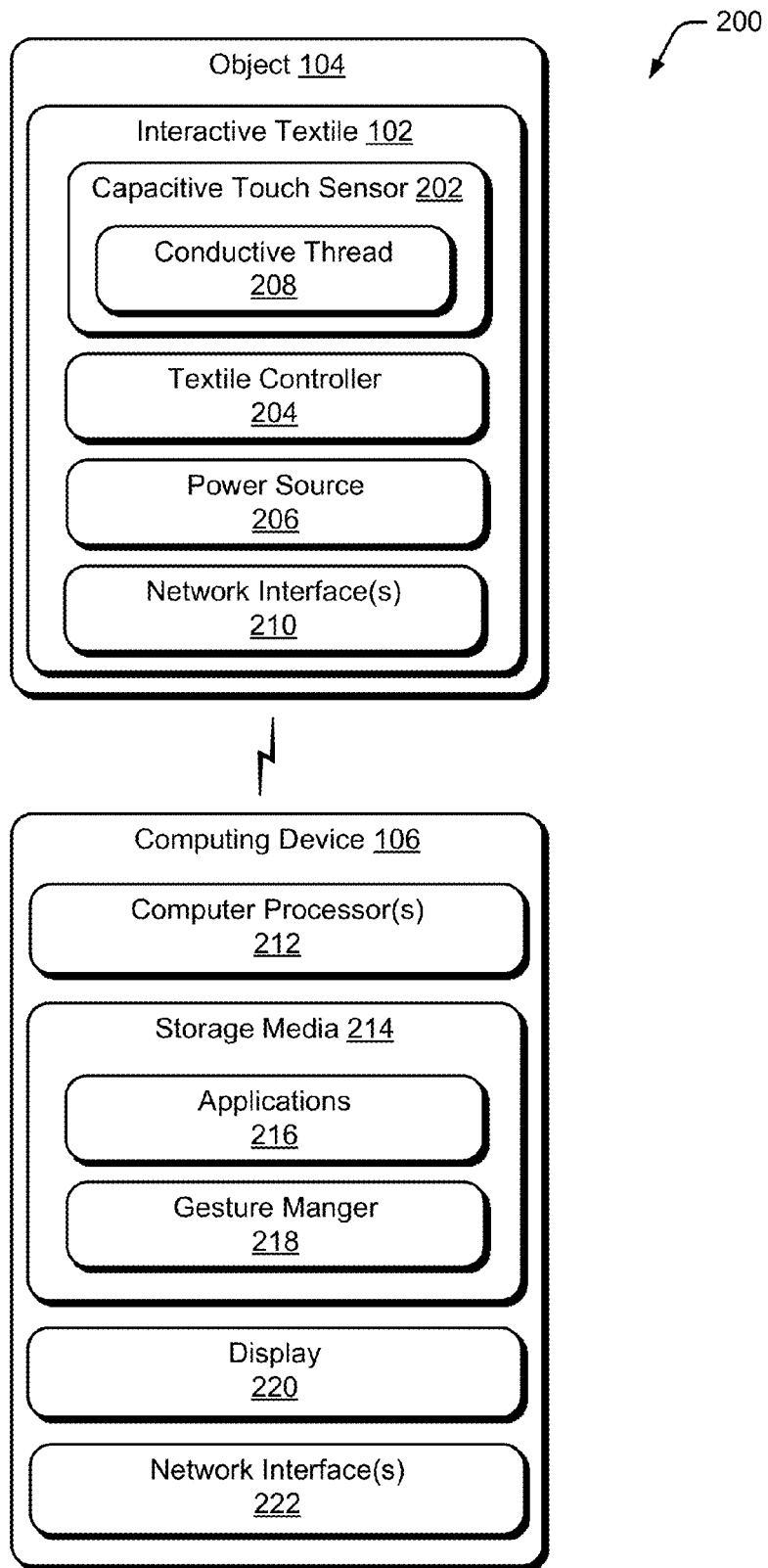


Fig. 2

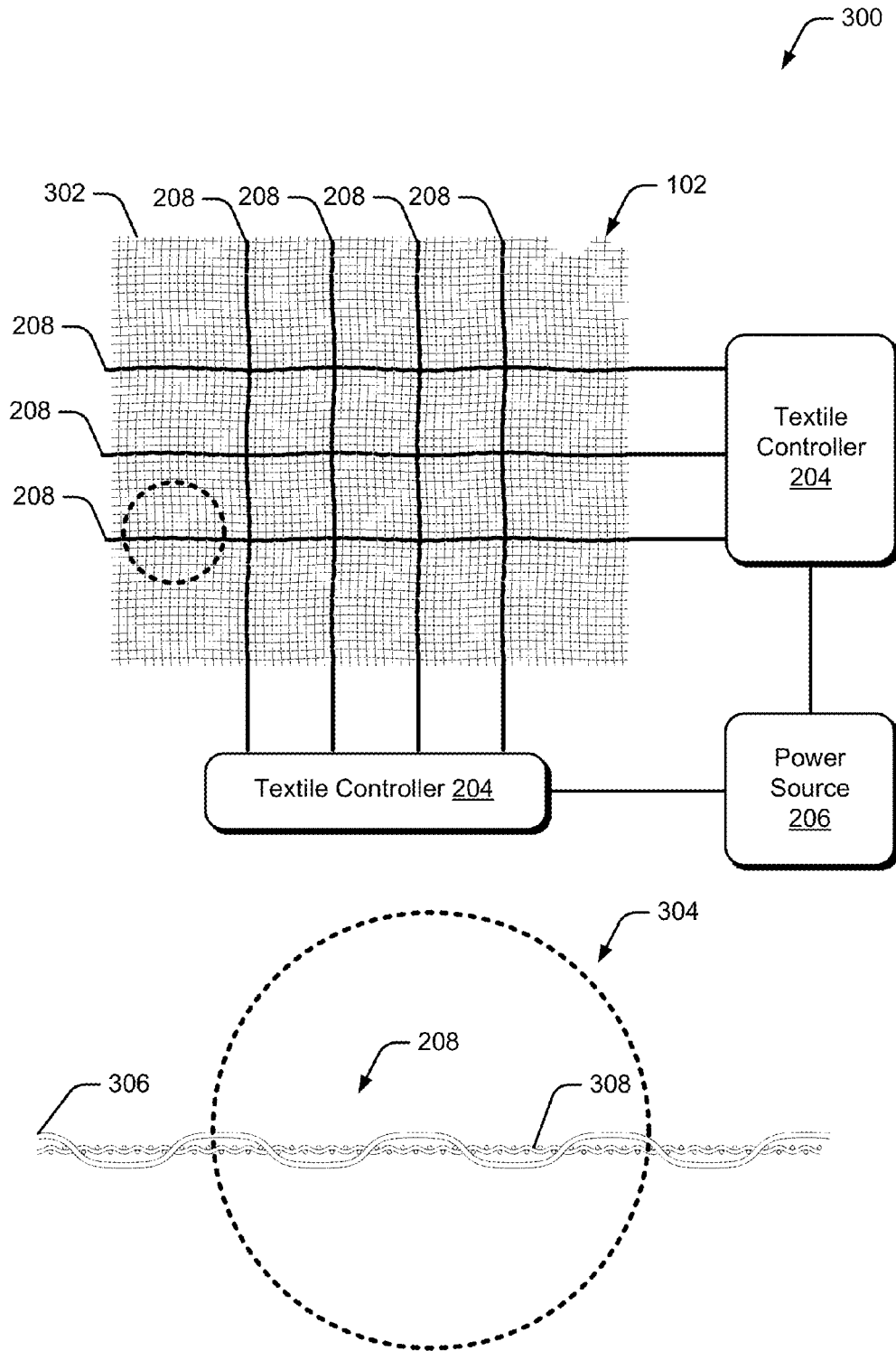


Fig. 3

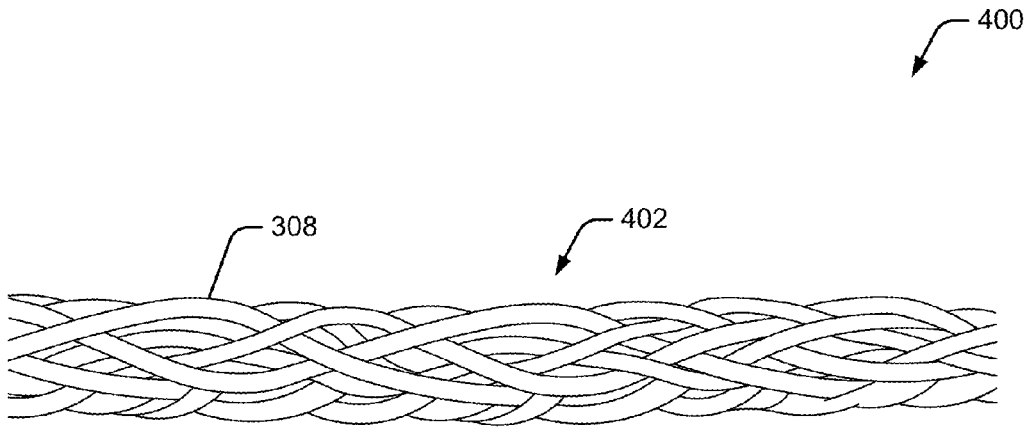


Fig. 4a

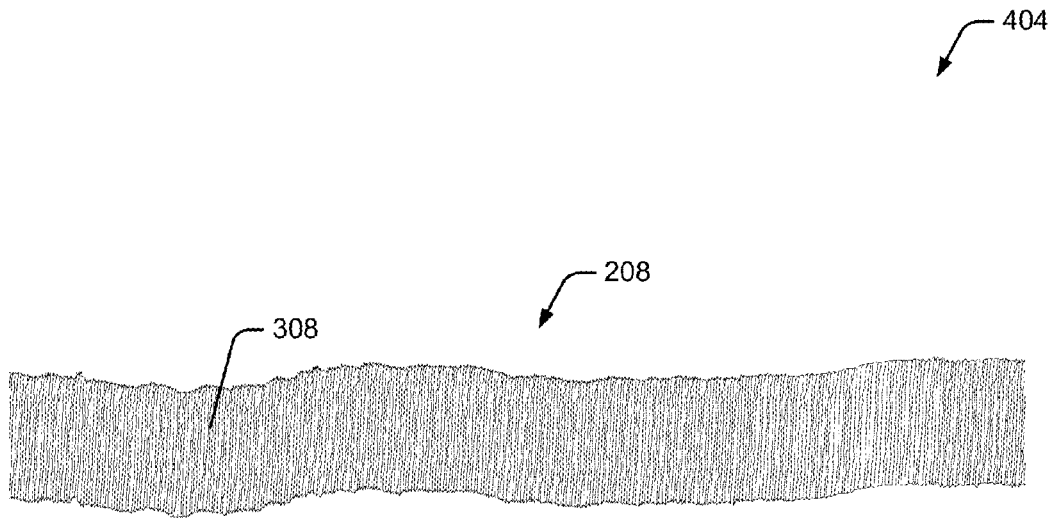


Fig. 4b

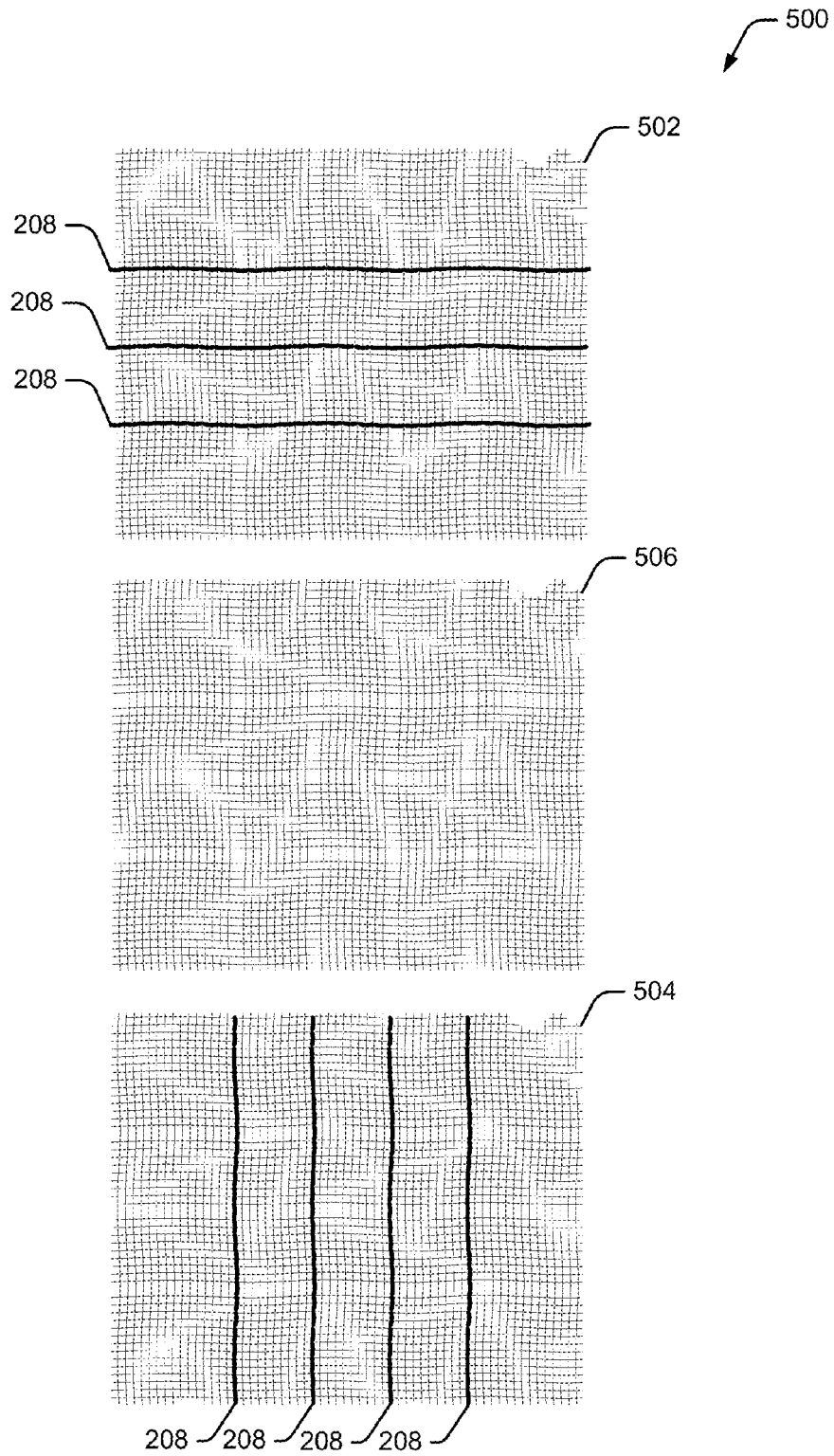


Fig. 5

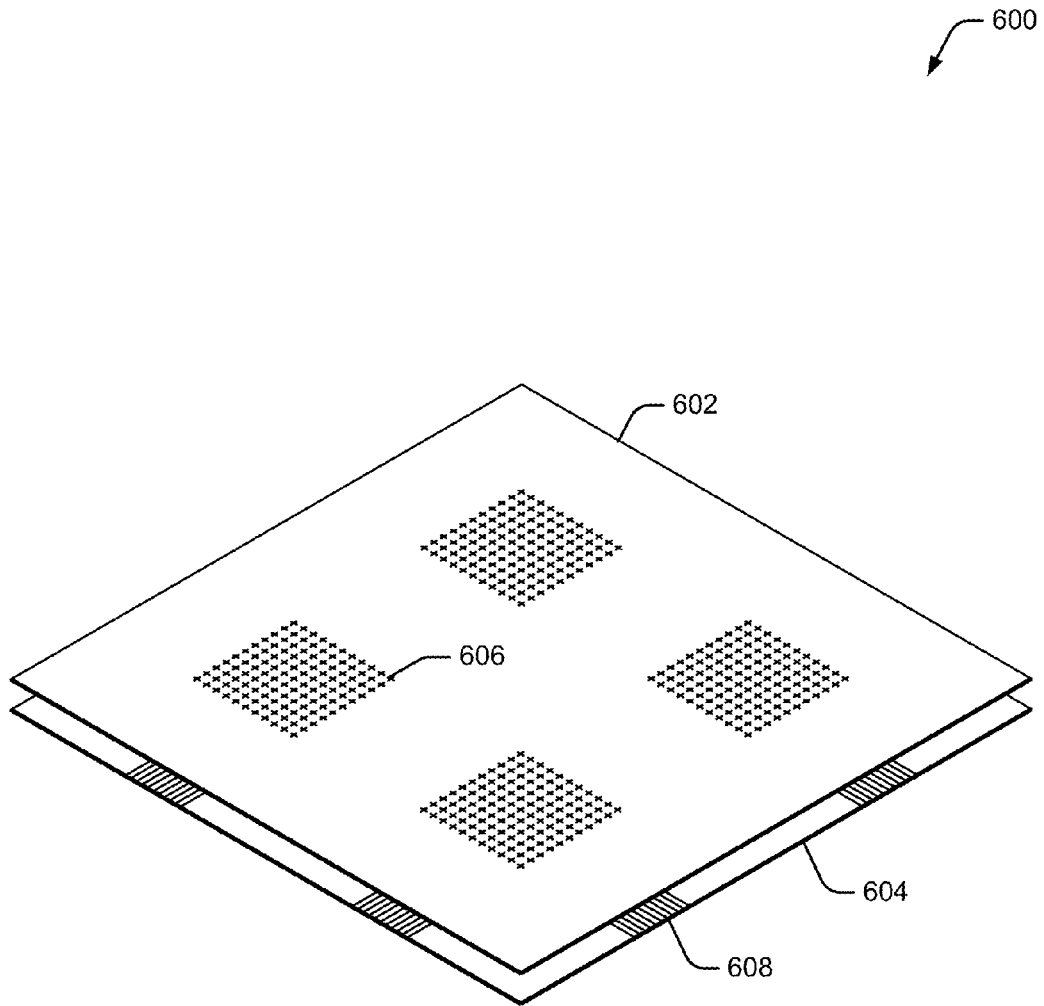


Fig. 6

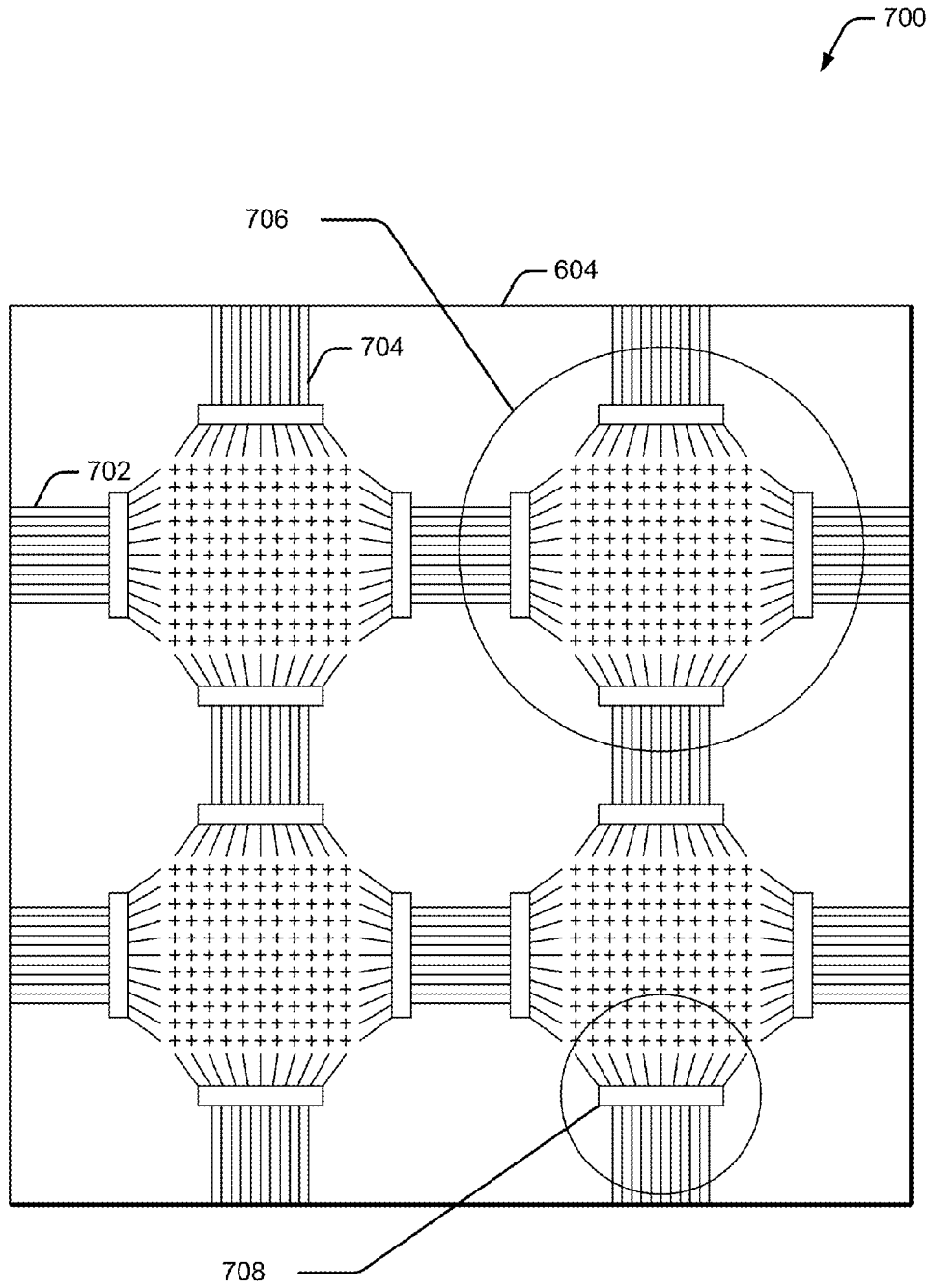


Fig. 7

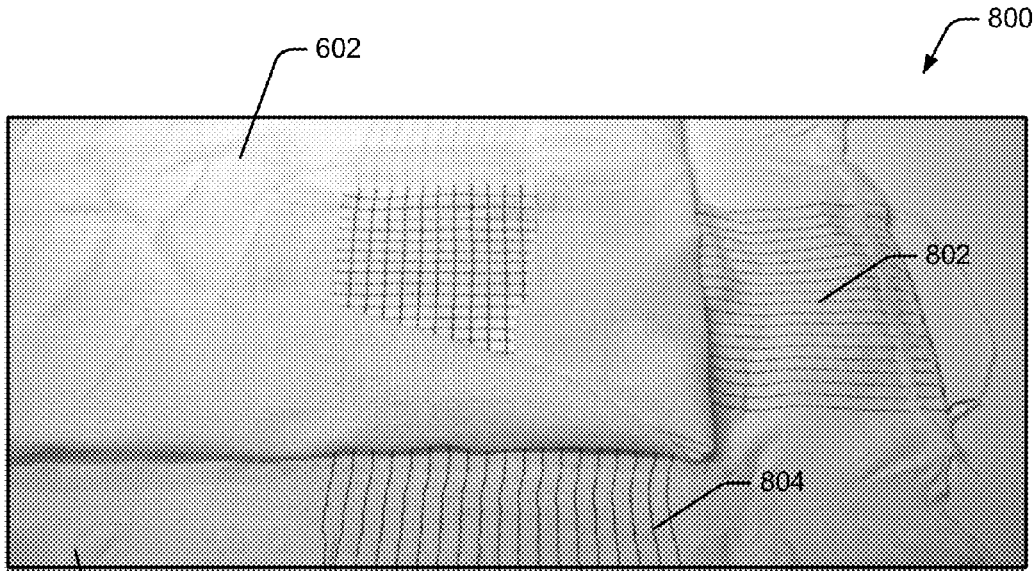


Fig. 8

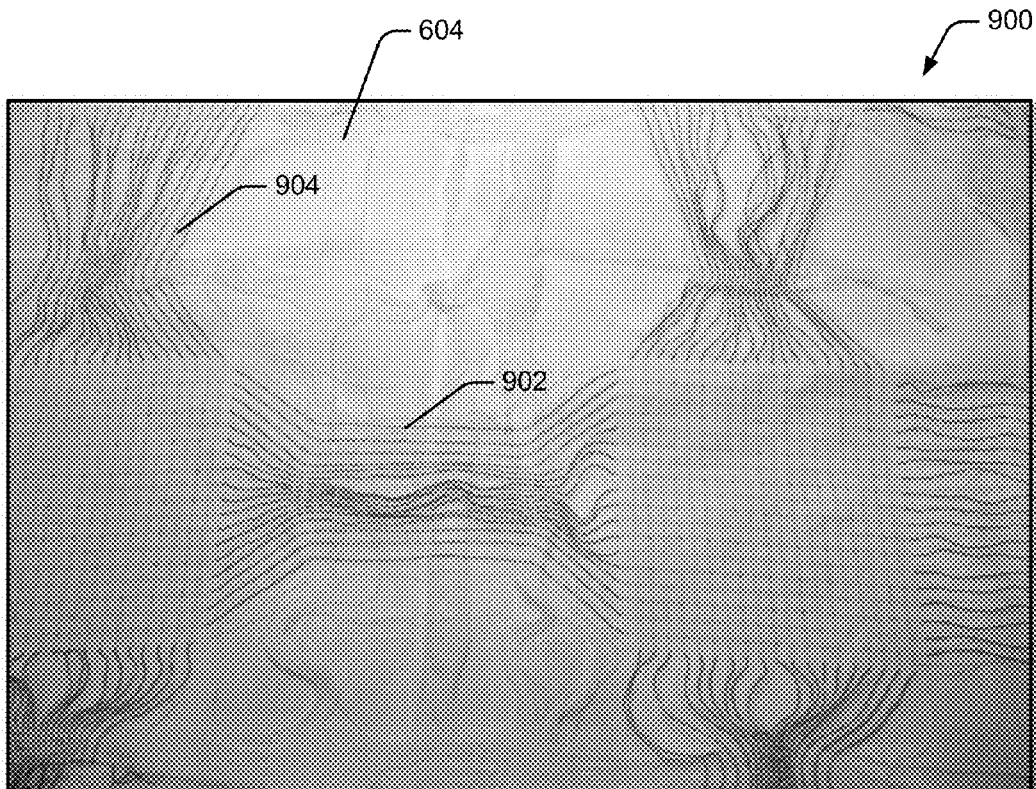


Fig. 9

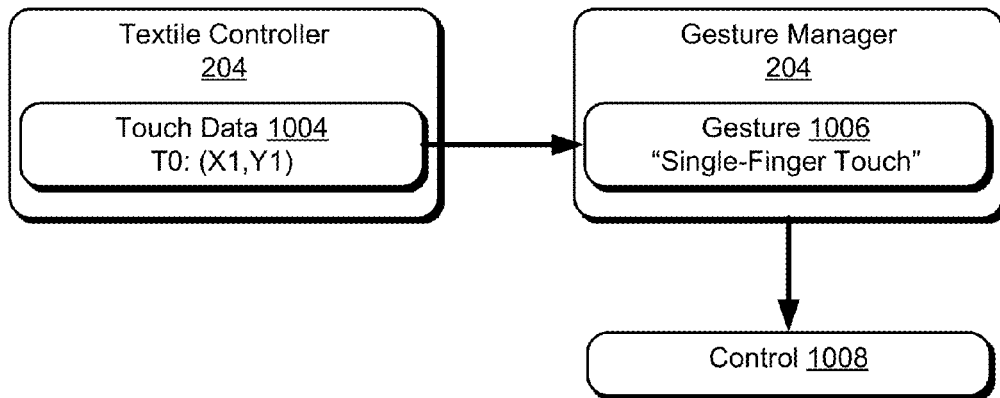
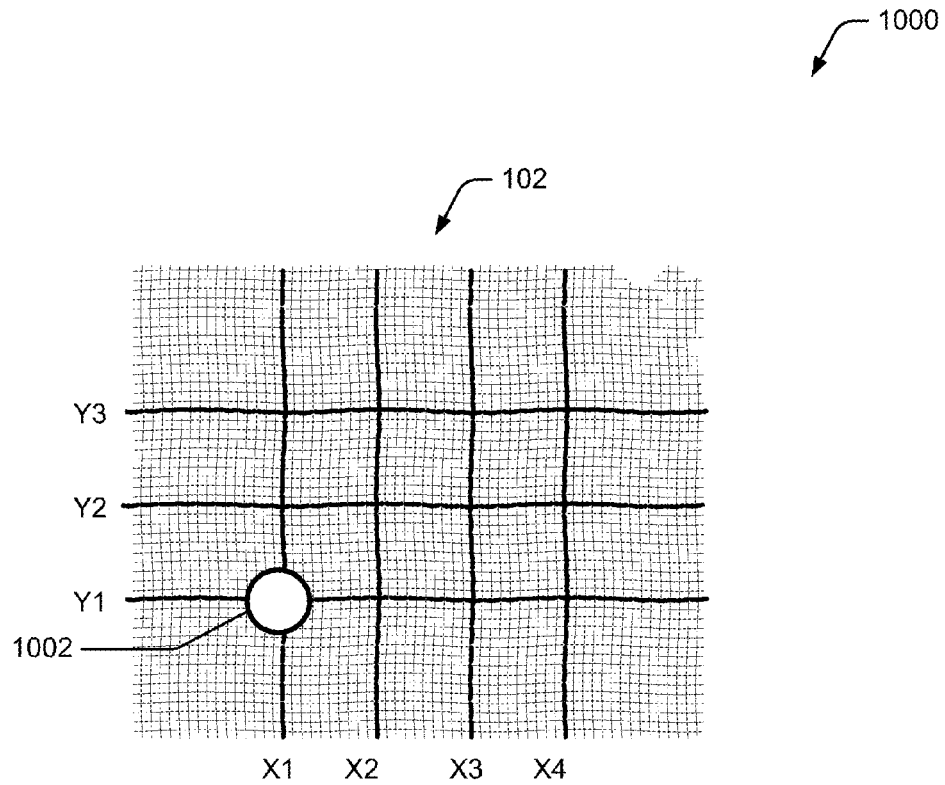


Fig. 10A

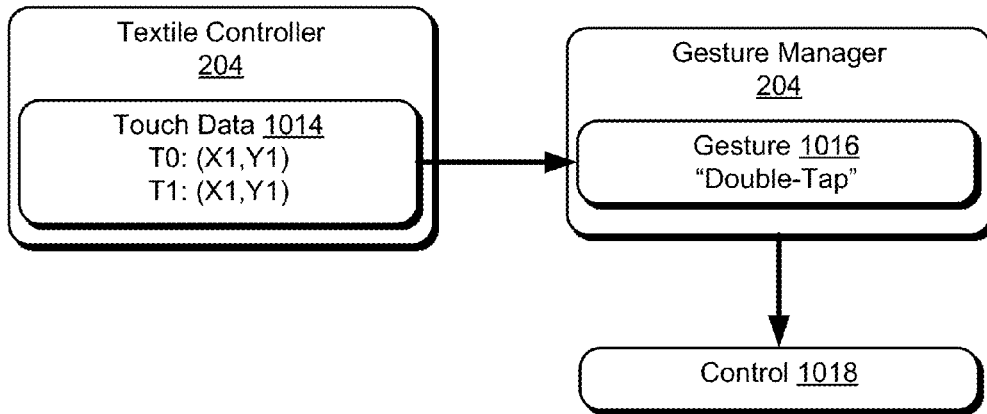
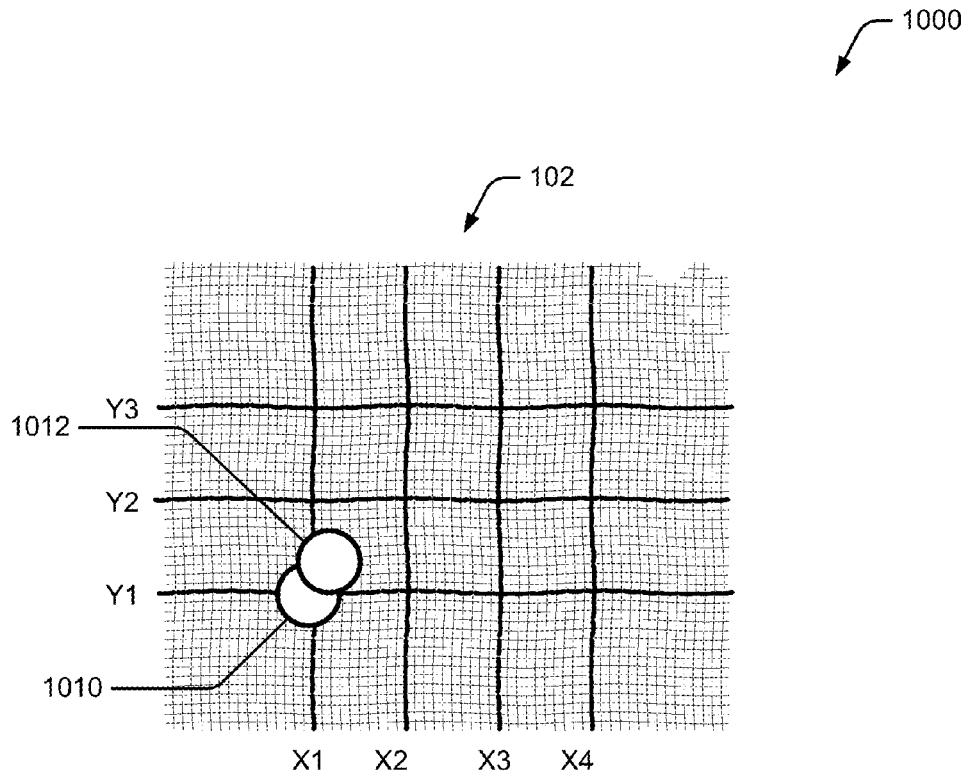


Fig. 10B

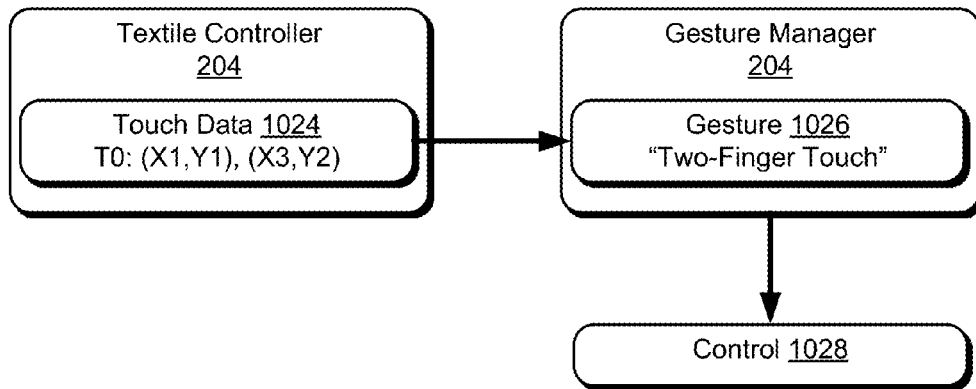
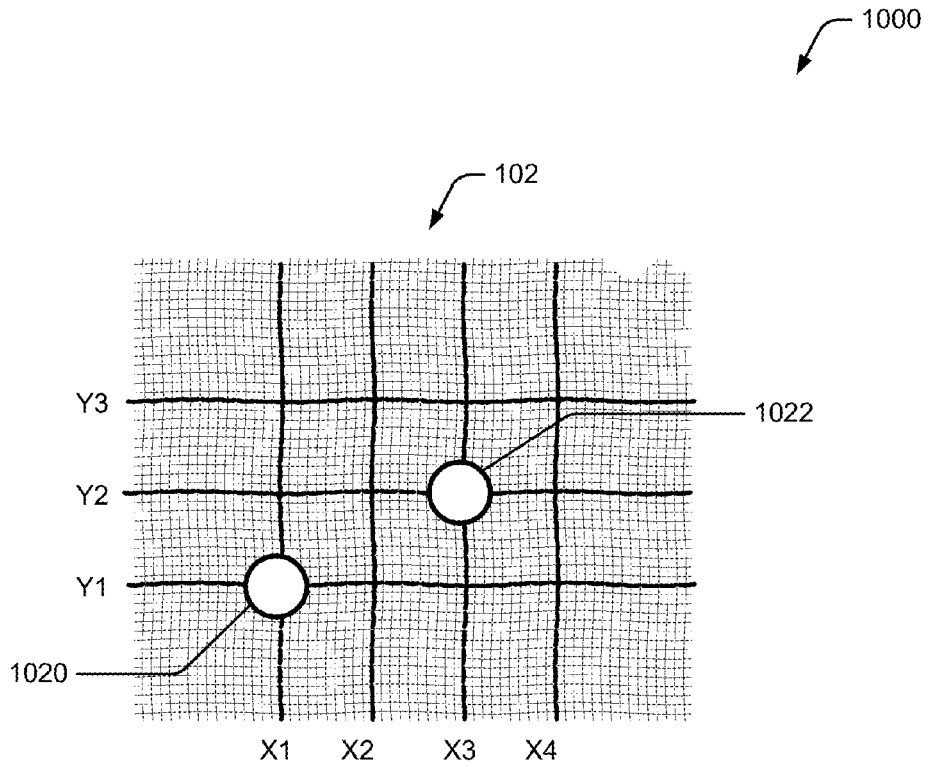


Fig. 10C

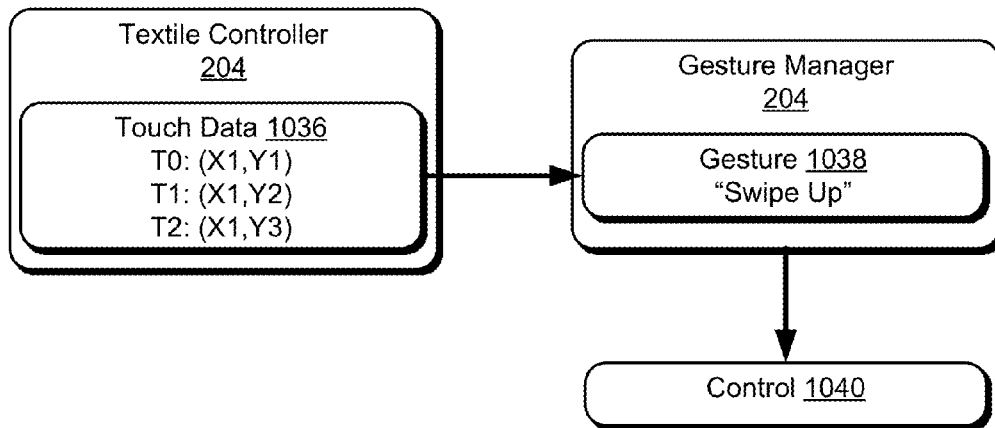
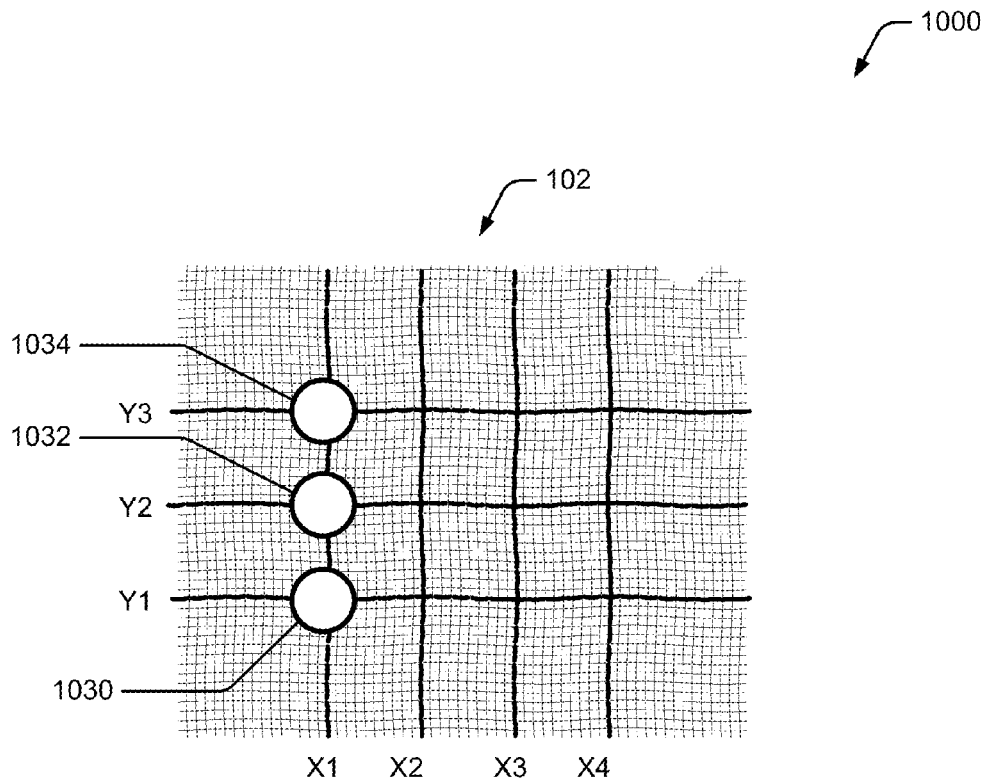


Fig. 10D

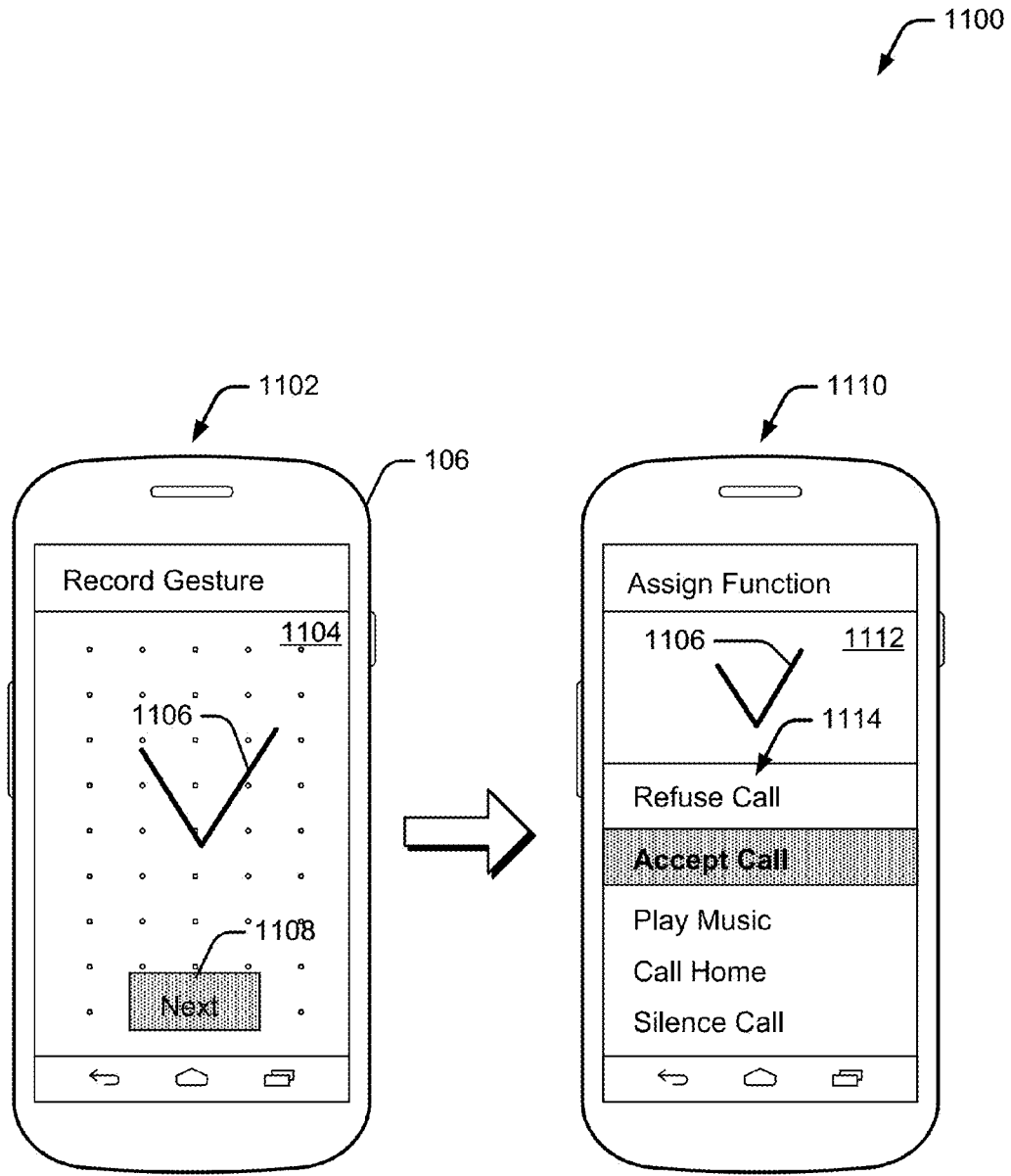


Fig. 11

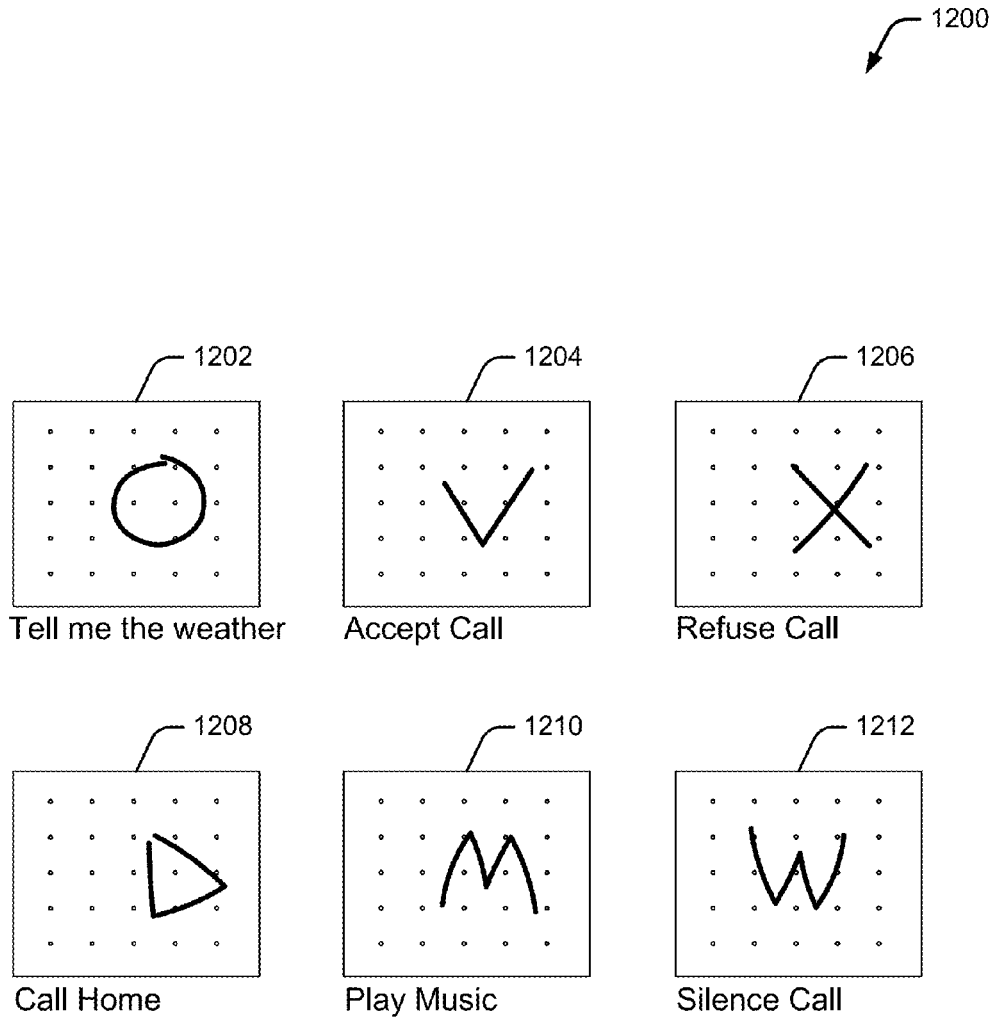


Fig. 12

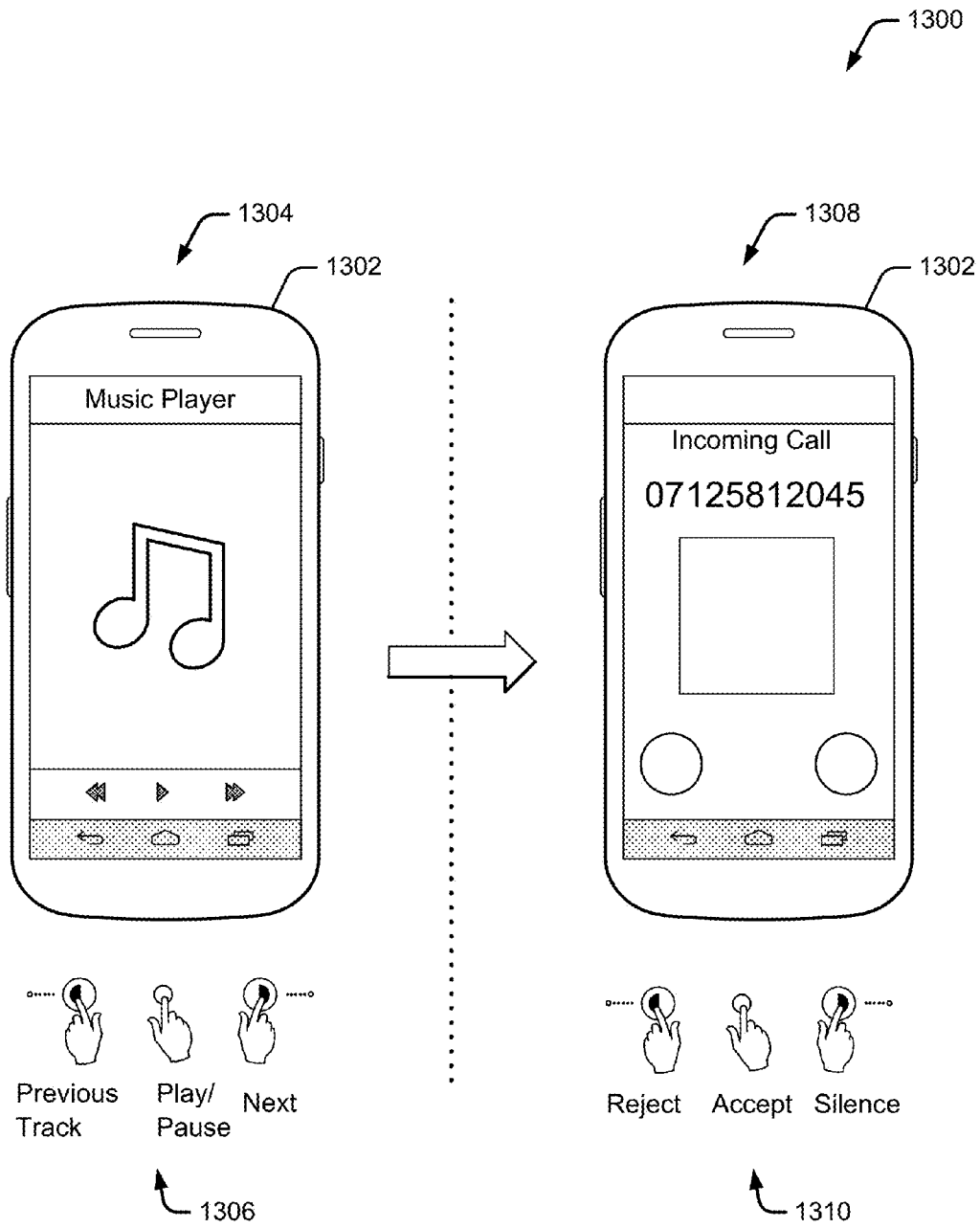


Fig. 13

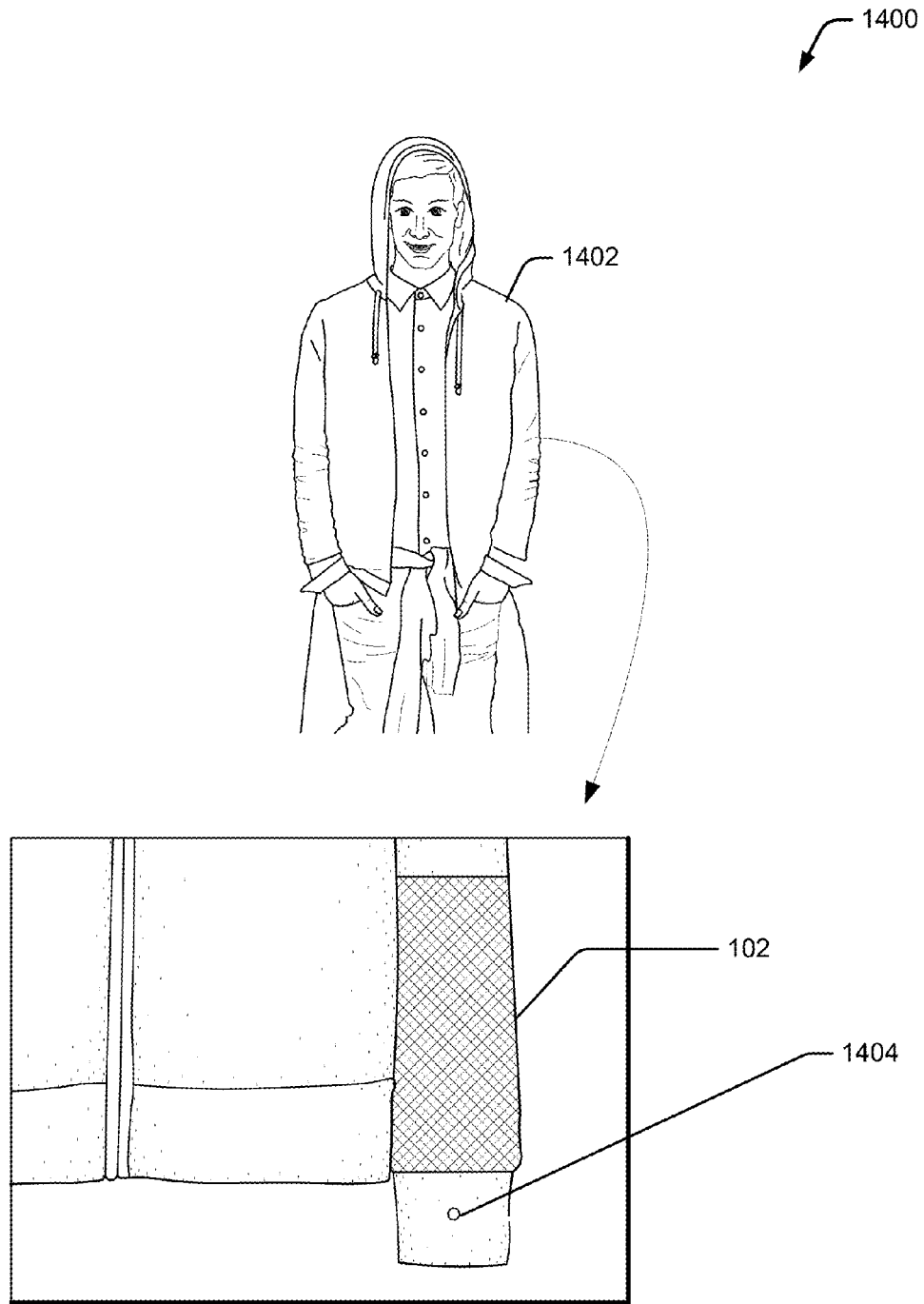


Fig. 14

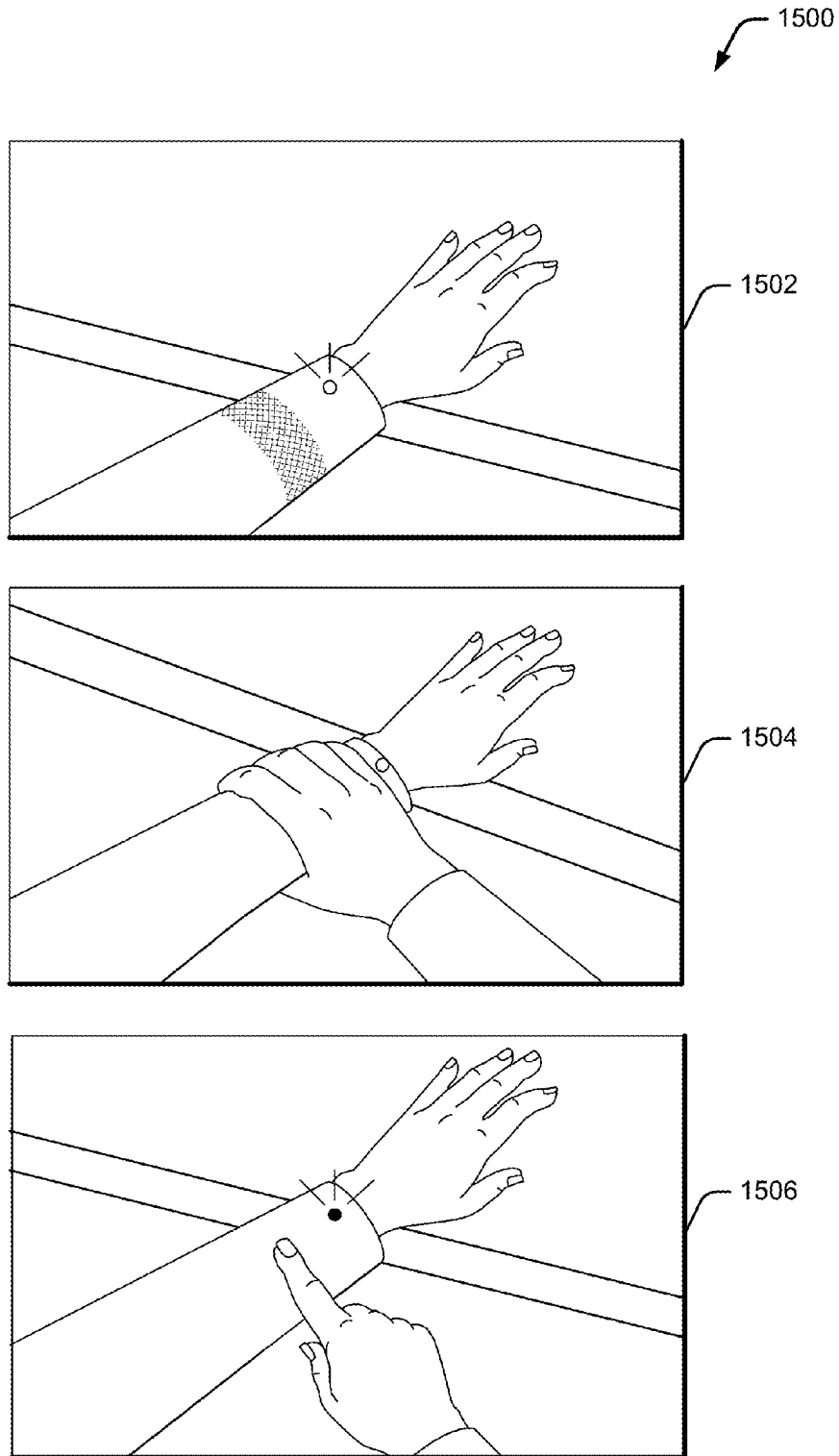


Fig. 15

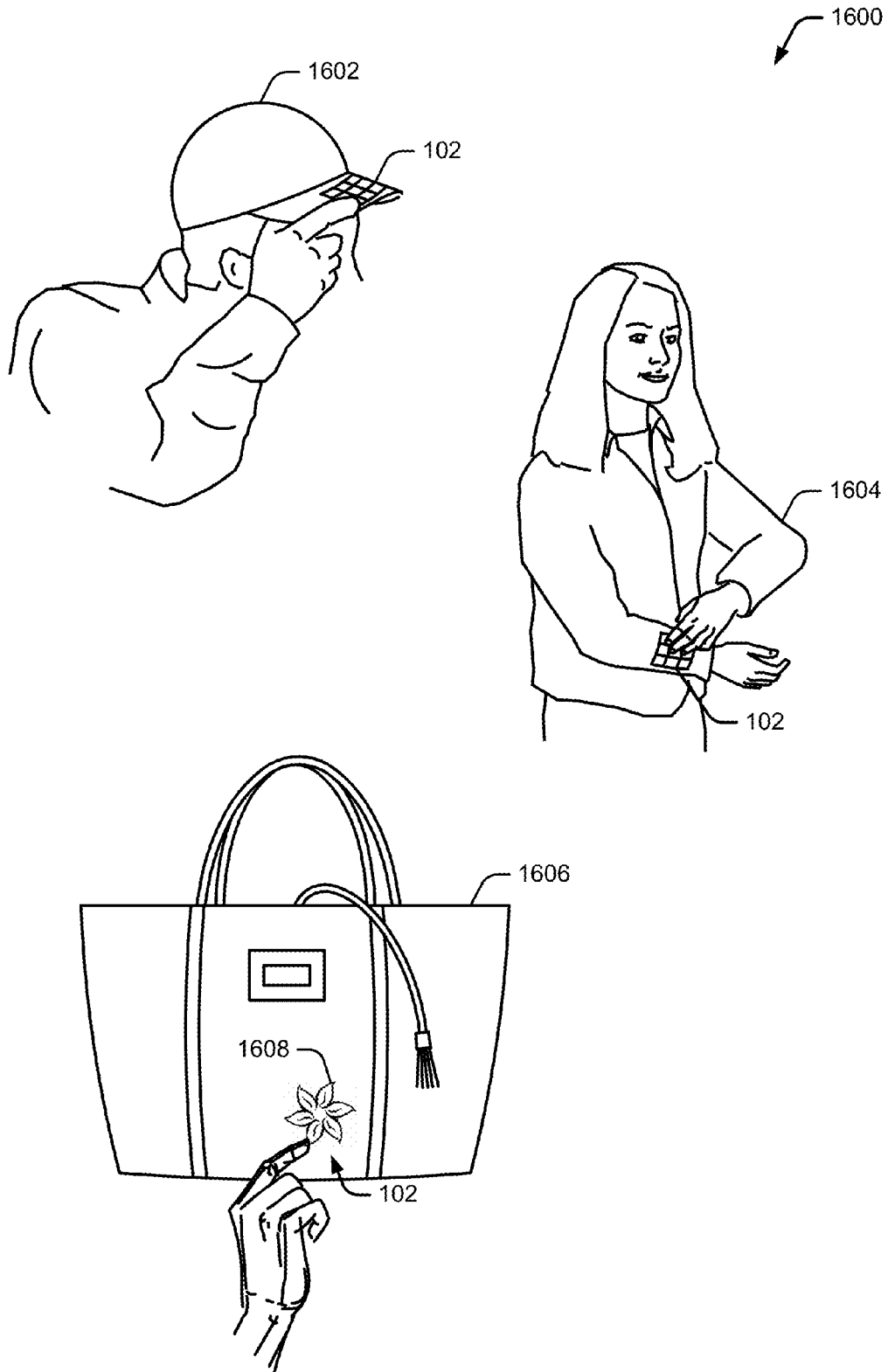


Fig. 16

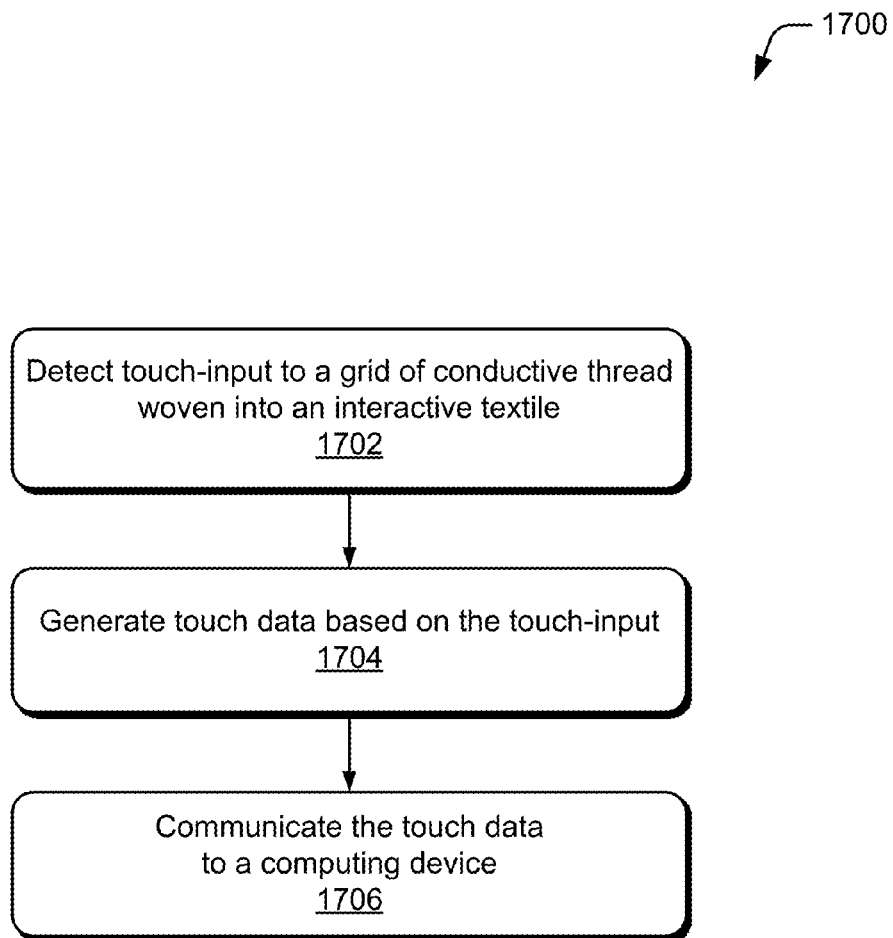


Fig. 17

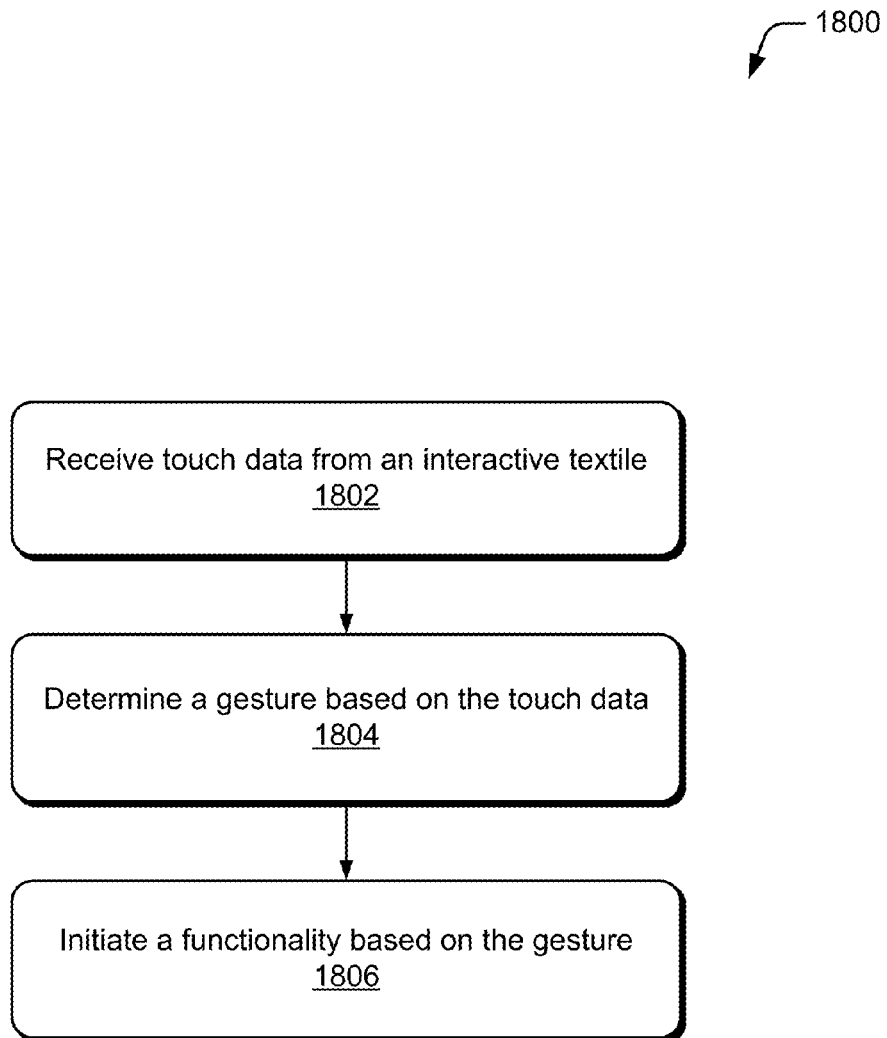


Fig. 18

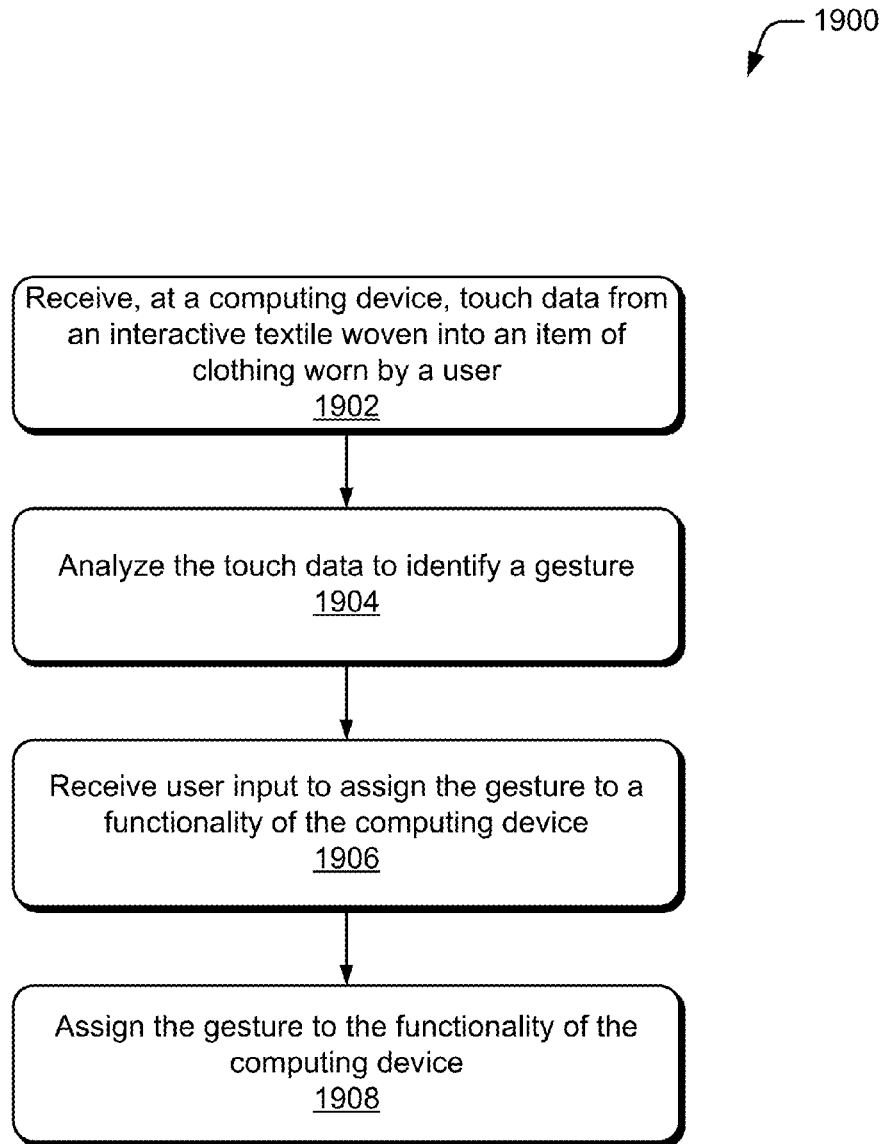


Fig. 19

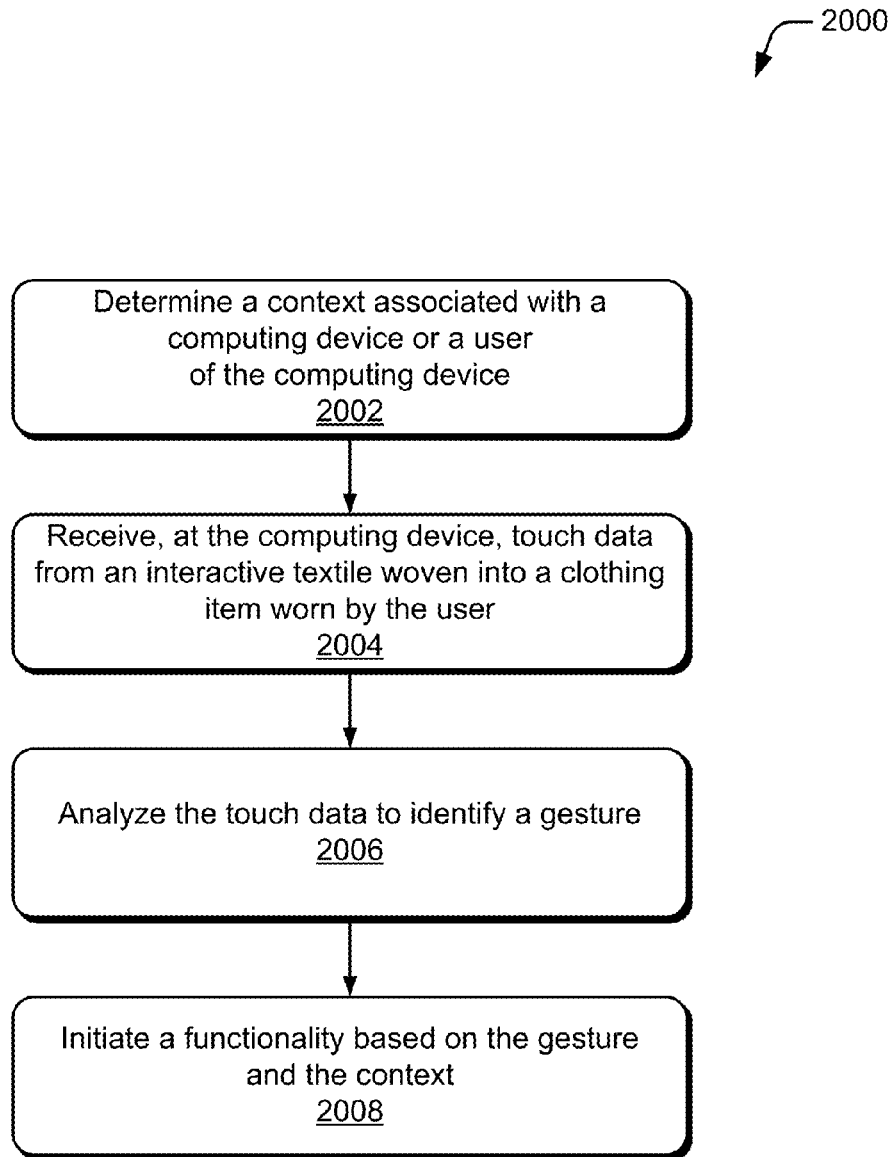


Fig. 20

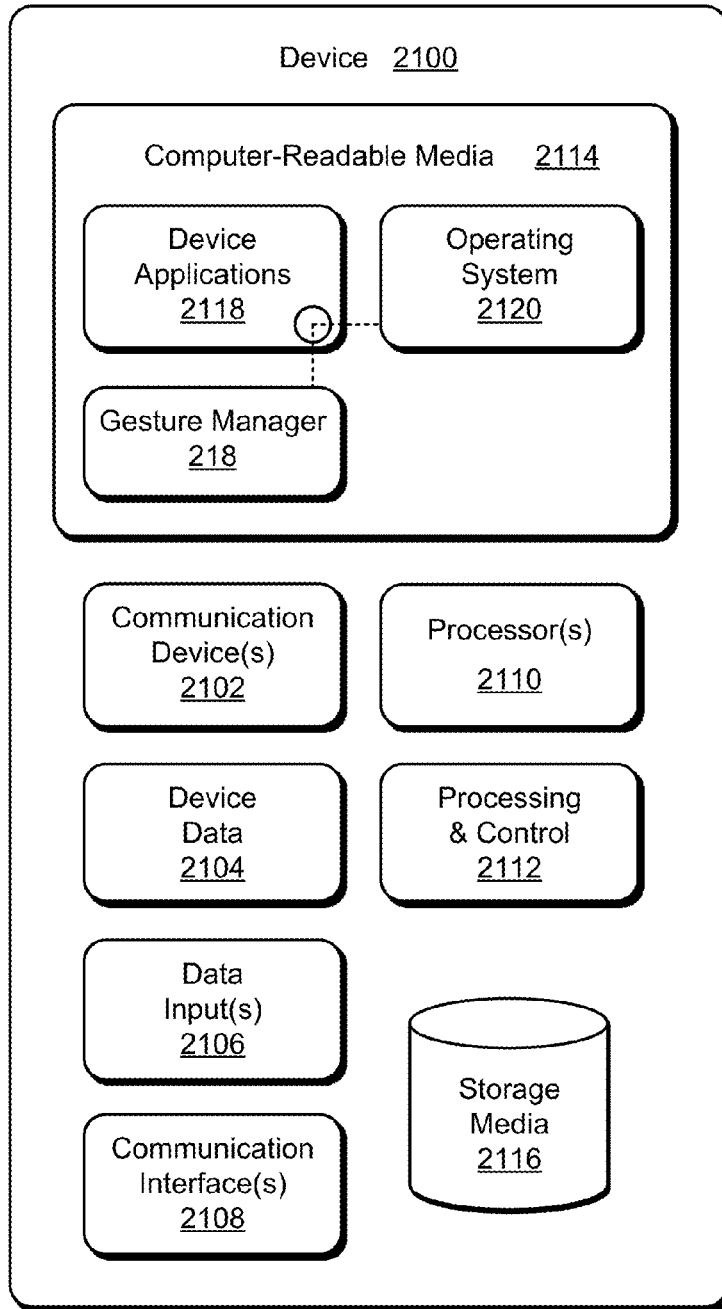


Fig. 21

TWO-LAYER INTERACTIVE TEXTILES

PRIORITY APPLICATION

[0001] This application is a non-provisional of and claims priority under 35 U.S.C. §119(e) to U.S. patent application Ser. No. 62/138,831 titled “Two-Layer Interactive Textiles,” filed Mar. 26, 2015, the disclosure of which is incorporated by reference herein in its entirety.

BACKGROUND

[0002] Currently, producing touch sensors can be complicated and expensive, especially if the touch sensor is intended to be light, flexible, or adaptive to various different kinds of use. Conventional touch pads, for example, are generally non-flexible and relatively costly to produce and to integrate into objects.

SUMMARY

[0003] This document describes two-layer interactive textiles. An interactive textile includes a grid of conductive thread woven into the interactive textile to form a capacitive touch sensor that is configured to detect touch-input. The interactive textile can process the touch-input to generate touch data that is useable to initiate functionality at various remote devices that are wirelessly coupled to the interactive textile. For example, the interactive textile may aid users in controlling volume on a stereo, pausing a movie playing on a television, or selecting a webpage on a desktop computer. Due to the flexibility of textiles, the interactive textile may be easily integrated within flexible objects, such as clothing, handbags, fabric casings, hats, and so forth.

[0004] In one or more implementations, the interactive textile includes a top textile layer and a bottom textile layer. Conductive threads are woven into the top textile layer and the bottom textile layer. When the top textile layer is combined with the bottom textile layer, the conductive threads from each layer form a capacitive touch sensor that is configured to detect touch-input. The bottom textile layer is not visible and couples the capacitive touch sensor to electronic components, such as a controller, a wireless interface, an output device (e.g., an LED, a display, or speaker), and so forth.

[0005] In one or more implementations, the conductive thread of the interactive textile includes a conductive core that includes at least one conductive wire and a cover layer constructed from flexible threads that covers the conductive core. The conductive core may be formed by twisting one or more flexible threads (e.g., silk threads, polyester threads, or cotton threads) with the conductive wire, or by wrapping flexible threads around the conductive wire. In one or more implementations, the conductive core is formed by braiding the conductive wire with flexible threads (e.g., silk). The cover layer may be formed by wrapping or braiding flexible threads around the conductive core. In one or more implementations, the conductive thread is implemented with a “double-braided” structure in which the conductive core is formed by braiding flexible threads with a conductive wire, and then braiding flexible threads around the braided conductive core.

[0006] In one or more implementations, a gesture manager is implemented at a computing device that is wirelessly coupled to the interactive textile. The gesture manager enables the user to create gestures and assign the gestures to various functionalities of the computing device. The gesture

manager can store mappings between the created gestures and the functionalities in a gesture library to enable the user to initiate a functionality, at a subsequent time, by inputting a gesture assigned to the functionality into the interactive textile.

[0007] In one or more implementations, the gesture manager is configured to select a functionality based on both a gesture to the interactive textile and a context of the computing device. The ability to recognize gestures based on context enables the user to invoke a variety of different functionalities using a subset of gestures. For example, for a first context, a first gesture may initiate a first functionality, whereas for a second context, the same first gesture may initiate a second functionality.

[0008] In one or more implementations, the interactive textile is coupled to one or more output devices (e.g., a light source, a speaker, or a display) that is integrated within the flexible object. The output device can be controlled to provide notifications initiated from the computing device and/or feedback to the user based on the user’s interactions with the interactive textile.

[0009] This summary is provided to introduce simplified concepts concerning two-layer interactive textiles, which is further described below in the Detailed Description. This summary is not intended to identify essential features of the claimed subject matter, nor is it intended for use in determining the scope of the claimed subject matter.

BRIEF DESCRIPTION OF THE DRAWINGS

[0010] Embodiments of techniques and devices for two-layer interactive textiles are described with reference to the following drawings. The same numbers are used throughout the drawings to reference like features and components:

[0011] FIG. 1 is an illustration of an example environment in which techniques using, and an objects including, an interactive textile may be embodied.

[0012] FIG. 2 illustrates an example system that includes an interactive textile and a gesture manager.

[0013] FIG. 3 illustrates an example of an interactive textile in accordance with one or more implementations.

[0014] FIG. 4a which illustrates an example of a conductive core for a conductive thread in accordance with one or more implementations.

[0015] FIG. 4b which illustrates an example of a conductive thread that includes a cover layer formed by wrapping flexible threads around a conductive core.

[0016] FIG. 5 illustrates an example of an interactive textile with multiple textile layers.

[0017] FIG. 6 illustrates an example of a two-layer interactive textile in accordance with one or more implementations.

[0018] FIG. 7 illustrates a more-detailed view of a second textile layer of a two-layer interactive textile in accordance with one or more implementations.

[0019] FIG. 8 illustrates an example of a second textile layer of a two-layer interactive textile in accordance with one or more implementations.

[0020] FIG. 9 illustrates an additional example of a second textile layer of a two-layer interactive textile in accordance with one or more implementations.

[0021] FIG. 10A illustrates an example of generating a control based on touch-input corresponding to a single-finger touch.

[0022] FIG. 10B illustrates an example of generating a control based on touch-input corresponding to a double-tap.

[0023] FIG. 10C illustrates an example of generating a control based on touch-input corresponding to a two-finger touch.

[0024] FIG. 10D illustrates an example of generating a control based on touch-input corresponding to a swipe up.

[0025] FIG. 11 illustrates an example of creating and assigning gestures to functionality of a computing device in accordance with one or more implementations.

[0026] FIG. 12 illustrates an example of a gesture library in accordance with one or more implementations.

[0027] FIG. 13 illustrates an example of contextual-based gestures to an interactive textile in accordance with one or more implementations.

[0028] FIG. 14 illustrates an example of an interactive textile that includes an output device in accordance with one or more implementations.

[0029] FIG. 15 illustrates implementation examples 1500 of interacting with an interactive textile and an output device in accordance with one or more implementations.

[0030] FIG. 16 illustrates various examples of interactive textiles integrated within flexible objects.

[0031] FIG. 17 illustrates an example method of generating touch data using an interactive textile.

[0032] FIG. 18 illustrates an example method of determining gestures usable to initiate functionality of a computing device in accordance with one or more implementations.

[0033] FIG. 19 illustrates an example method 1900 of assigning a gesture to a functionality of a computing device in accordance with one or more implementations.

[0034] FIG. 20 illustrates an example method 2300 of initiating a functionality of a computing device based on a gesture and a context in accordance with one or more implementations.

[0035] FIG. 21 illustrates various components of an example computing system that can be implemented as any type of client, server, and/or computing device as described with reference to the previous FIGS. 1-20 to implement two-layer interactive textiles.

DETAILED DESCRIPTION

Overview

[0036] Currently, producing touch sensors can be complicated and expensive, especially if the touch sensor is intended to be light, flexible, or adaptive to various different kinds of use. This document describes techniques using, and objects embodying, interactive textiles which are configured to sense multi-touch-input. To enable the interactive textiles to sense multi-touch-input, a grid of conductive thread is woven into the interactive textile to form a capacitive touch sensor that can detect touch-input. The interactive textile can process the touch-input to generate touch data that is useable to initiate functionality at various remote devices. For example, the interactive textiles may aid users in controlling volume on a stereo, pausing a movie playing on a television, or selecting a webpage on a desktop computer. Due to the flexibility of textiles, the interactive textile may be easily integrated within flexible objects, such as clothing, handbags, fabric casings, hats, and so forth.

[0037] In one or more implementations, the interactive textile includes a top textile layer and a bottom textile layer. Conductive threads are woven into the top textile layer and the bottom textile layer. When the top textile layer is combined with the bottom textile layer, the conductive threads

from each layer form a capacitive touch sensor that is configured to detect touch-input. The bottom textile layer is not visible and couples the capacitive through sensor to electronic components, such as a controller, a wireless interface, an output device (e.g., an LED, a display, or speaker), and so forth.

[0038] In one or more implementations, the conductive thread of the interactive textile includes a conductive core that includes at least one conductive wire and a cover layer constructed from flexible threads that covers the conductive core. The conductive core may be formed by twisting one or more flexible threads (e.g., silk threads, polyester threads, or cotton threads) with the conductive wire, or by wrapping flexible threads around the conductive wire. In one or more implementations, the conductive core is formed by braiding the conductive wire with flexible threads (e.g., silk). The cover layer may be formed by wrapping or braiding flexible threads around the conductive core. In one or more implementations, the conductive thread is implemented with a “double-braided” structure in which the conductive core is formed by braiding flexible threads with a conductive wire, and then braiding flexible threads around the braided conductive core.

[0039] In one or more implementations, a gesture manager is implemented at a computing device that is wirelessly coupled to the interactive textile. The gesture manager enables the user to create gestures and assign the gestures to various functionalities of the computing device. The gesture manager can store mappings between the created gestures and the functionalities in a gesture library to enable the user to initiate a functionality, at a subsequent time, by inputting a gesture assigned to the functionality into the interactive textile.

[0040] In one or more implementations, the gesture manager is configured to select a functionality based on both a gesture to the interactive textile and a context of the computing device. The ability to recognize gestures based on context enables the user to invoke a variety of different functionalities using a subset of gestures. For example, for a first context, a first gesture may initiate a first functionality, whereas for a second context, the same first gesture may initiate a second functionality.

[0041] In one or more implementations, the interactive textile is coupled to one or more output devices (e.g., a light source, a speaker, or a display) that is integrated within the flexible object. The output device can be controlled to provide notifications initiated from the computing device and/or feedback to the user based on the user’s interactions with the interactive textile.

Example Environment

[0042] FIG. 1 is an illustration of an example environment 100 in which techniques using, and objects including, an interactive textile may be embodied. Environment 100 includes an interactive textile 102, which is shown as being integrated within various objects 104. Interactive textile 102 is a textile that is configured to sense multi-touch input. As described herein, a textile corresponds to any type of flexible woven material consisting of a network of natural or artificial fibers, often referred to as thread or yarn. Textiles may be formed by weaving, knitting, crocheting, knotting, or pressing threads together.

[0043] In environment 100, objects 104 include “flexible” objects, such as a shirt 104-1, a hat 104-2, and a handbag 104-3. It is to be noted, however, that interactive textile 102

may be integrated within any type of flexible object made from fabric or a similar flexible material, such as articles of clothing, blankets, shower curtains, towels, sheets, bed spreads, or fabric casings of furniture, to name just a few. As discussed in more detail below, interactive textile **102** may be integrated within flexible objects **104** in a variety of different ways, including weaving, sewing, gluing, and so forth.

[0044] In this example, objects **104** further include “hard” objects, such as a plastic cup **104-4** and a hard smart phone casing **104-5**. It is to be noted, however, that hard objects **104** may include any type of “hard” or “rigid” object made from non-flexible or semi-flexible materials, such as plastic, metal, aluminum, and so on. For example, hard objects **104** may also include plastic chairs, water bottles, plastic balls, or car parts, to name just a few. Interactive textile **102** may be integrated within hard objects **104** using a variety of different manufacturing processes. In one or more implementations, injection molding is used to integrate interactive textiles **102** into hard objects **104**.

[0045] Interactive textile **102** enables a user to control object **104** that the interactive textile **102** is integrated with, or to control a variety of other computing devices **106** via a network **108**. Computing devices **106** are illustrated with various non-limiting example devices: server **106-1**, smart phone **106-2**, laptop **106-3**, computing spectacles **106-4**, television **106-5**, camera **106-6**, tablet **106-7**, desktop **106-8**, and smart watch **106-9**, though other devices may also be used, such as home automation and control systems, sound or entertainment systems, home appliances, security systems, networks, and e-readers. Note that computing device **106** can be wearable (e.g., computing spectacles and smart watches), non-wearable but mobile (e.g., laptops and tablets), or relatively immobile (e.g., desktops and servers).

[0046] Network **108** includes one or more of many types of wireless or partly wireless communication networks, such as a local-area-network (LAN), a wireless local-area-network (WLAN), a personal-area-network (PAN), a wide-area-network (WAN), an intranet, the Internet, a peer-to-peer network, point-to-point network, a mesh network, and so forth.

[0047] Interactive textile **102** can interact with computing devices **106** by transmitting touch data through network **108**. Computing device **106** uses the touch data to control computing device **106** or applications at computing device **106**. As an example, consider that interactive textile **102** integrated at shirt **104-1** may be configured to control the user’s smart phone **106-2** in the user’s pocket, television **106-5** in the user’s home, smart watch **106-9** on the user’s wrist, or various other appliances in the user’s house, such as thermostats, lights, music, and so forth. For example, the user may be able to swipe up or down on interactive textile **102** integrated within the user’s shirt **104-1** to cause the volume on television **106-5** to go up or down, to cause the temperature controlled by a thermostat in the user’s house to increase or decrease, or to turn on and off lights in the user’s house. Note that any type of touch, tap, swipe, hold, or stroke gesture may be recognized by interactive textile **102**.

[0048] In more detail, consider FIG. 2 which illustrates an example system **200** that includes an interactive textile and a gesture manager. In system **200**, interactive textile **102** is integrated in an object **104**, which may be implemented as a flexible object (e.g., shirt **104-1**, hat **104-2**, or handbag **104-3**) or a hard object (e.g., plastic cup **104-4** or smart phone casing **104-5**).

[0049] Interactive textile **102** is configured to sense multi-touch-input from a user when one or more fingers of the user’s hand touch interactive textile **102**. Interactive textile **102** may also be configured to sense full-hand touch input from a user, such as when an entire hand of the user touches or swipes interactive textile **102**. To enable this, interactive textile **102** includes a capacitive touch sensor **202**, a textile controller **204**, and a power source **206**.

[0050] Capacitive touch sensor **202** is configured to sense touch-input when an object, such as a user’s finger, hand, or a conductive stylus, approaches or makes contact with capacitive touch sensor **202**. Unlike conventional hard touch pads, capacitive touch sensor **202** uses a grid of conductive thread **208** woven into interactive textile **102** to sense touch-input. Thus, capacitive touch sensor **202** does not alter the flexibility of interactive textile **102**, which enables interactive textile **102** to be easily integrated within objects **104**.

[0051] Power source **206** is coupled to textile controller **204** to provide power to textile controller **204**, and may be implemented as a small battery. Textile controller **204** is coupled to capacitive touch sensor **202**. For example, wires from the grid of conductive threads **208** may be connected to textile controller **204** using flexible PCB, creping, gluing with conductive glue, soldering, and so forth.

[0052] In one or more implementations, interactive textile **102** (or object **104**) may also include one or more output devices, such as light sources (e.g., LED’s), displays, or speakers. In this case, the output devices may also be connected to textile controller **204** to enable textile controller **204** to control their output.

[0053] Textile controller **204** is implemented with circuitry that is configured to detect the location of the touch-input on the grid of conductive thread **208**, as well as motion of the touch-input. When an object, such as a user’s finger, touches capacitive touch sensor **202**, the position of the touch can be determined by controller **204** by detecting a change in capacitance on the grid of conductive thread **208**. Textile controller **204** uses the touch-input to generate touch data usable to control computing device **102**. For example, the touch-input can be used to determine various gestures, such as single-finger touches (e.g., touches, taps, and holds), multi-finger touches (e.g., two-finger touches, two-finger taps, two-finger holds, and pinches), single-finger and multi-finger swipes (e.g., swipe up, swipe down, swipe left, swipe right), and full-hand interactions (e.g., touching the textile with a user’s entire hand, covering textile with the user’s entire hand, pressing the textile with the user’s entire hand, palm touches, and rolling, twisting, or rotating the user’s hand while touching the textile). Capacitive touch sensor **202** may be implemented as a self-capacitance sensor, or a projective capacitance sensor, which is discussed in more detail below.

[0054] Object **104** may also include network interfaces **210** for communicating data, such as touch data, over wired, wireless, or optical networks to computing devices **106**. By way of example and not limitation, network interfaces **210** may communicate data over a local-area-network (LAN), a wireless local-area-network (WLAN), a personal-area-network (PAN) (e.g., Bluetooth™), a wide-area-network (WAN), an intranet, the Internet, a peer-to-peer network, point-to-point network, a mesh network, and the like (e.g., through network **108** of FIG. 1).

[0055] In this example, computing device **106** includes one or more computer processors **212** and computer-readable storage media (storage media) **214**. Storage media **214**

includes applications 216 and/or an operating system (not shown) embodied as computer-readable instructions executable by computer processors 212 to provide, in some cases, functionalities described herein. Storage media 214 also includes a gesture manager 218 (described below).

[0056] Computing device 106 may also include a display 220 and network interfaces 222 for communicating data over wired, wireless, or optical networks. For example, network interfaces 222 can receive touch data sensed by interactive textile 102 from network interfaces 210 of object 104. By way of example and not limitation, network interface 222 may communicate data over a local-area-network (LAN), a wireless local-area-network (WLAN), a personal-area-network (PAN) (e.g., Bluetooth™), a wide-area-network (WAN), an intranet, the Internet, a peer-to-peer network, point-to-point network, a mesh network, and the like.

[0057] Gesture manager 218 is capable of interacting with applications 216 and interactive textile 102 effective to activate various functionalities associated with computing device 106 and/or applications 216 through touch-input (e.g., gestures) received by interactive textile 102. Gesture manager 218 may be implemented at a computing device 106 that is local to object 104, or remote from object 104.

[0058] Having discussed a system in which interactive textile 102 can be implemented, now consider a more-detailed discussion of interactive textile 102.

[0059] FIG. 3 illustrates an example 300 of interactive textile 102 in accordance with one or more implementations. In this example, interactive textile 102 includes non-conductive threads 302 woven with conductive threads 208 to form interactive textile 102. Non-conductive threads 302 may correspond to any type of non-conductive thread, fiber, or fabric, such as cotton, wool, silk, nylon, polyester, and so forth.

[0060] At 304, a zoomed-in view of conductive thread 208 is illustrated. Conductive thread 208 includes a conductive wire 306 twisted with a flexible thread 308. Twisting conductive wire 306 with flexible thread 308 causes conductive thread 208 to be flexible and stretchy, which enables conductive thread 208 to be easily woven with non-conductive threads 302 to form interactive textile 102.

[0061] In one or more implementations, conductive wire 306 is a thin copper wire. It is to be noted, however, that conductive wire 306 may also be implemented using other materials, such as silver, gold, or other materials coated with a conductive polymer. Flexible thread 308 may be implemented as any type of flexible thread or fiber, such as cotton, wool, silk, nylon, polyester, and so forth.

[0062] In one or more implementations, conductive thread 208 includes a conductive core that includes at least one conductive wire 306 (e.g., one or more copper wires) and a cover layer, configured to cover the conductive core, that is constructed from flexible threads 308. In some cases, conductive wire 306 of the conductive core is insulated. Alternately, conductive wire 306 of the conductive core is not insulated.

[0063] In one or more implementations, the conductive core may be implemented using a single, straight, conductive wire 306. Alternately, the conductive core may be implemented using a conductive wire 306 and one or more flexible threads 308. For example, the conductive core may be formed by twisting one or more flexible threads 308 (e.g., silk threads, polyester threads, or cotton threads) with conductive wire 306 (e.g., as shown at 304 of FIG. 3), or by wrapping flexible threads 308 around conductive wire 306.

[0064] In one or more implementations, the conductive core includes flexible threads 308 braided with conductive wire 306. As an example, consider FIG. 4a which illustrates an example 400 of a conductive core 402 for a conductive thread in accordance with one or more implementations. In this example, conductive core 402 is formed by braiding conductive wire 306 (not pictured) with flexible threads 308. A variety of different types of flexible threads 308 may be utilized to braid with conductive wire 306, such as polyester or cotton, in order to form the conductive core.

[0065] In one or more implementations, however, silk threads are used for the braided construction of the conductive core. Silk threads are slightly twisted which enables the silk threads to “grip” or hold on to conductive wire 306. Thus, using silk threads may increase the speed at which the braided conductive core can be manufactured. In contrast, a flexible thread like polyester is slippery, and thus does not “grip” the conductive wire as well as silk. Thus, a slippery thread is more difficult to braid with the conductive wire, which may slow down the manufacturing process.

[0066] An additional benefit of using silk threads to create the braided conductive core is that silk is both thin and strong, which enables the manufacture of a thin conductive core that will not break during the interaction textile weaving process. A thin conductive core is beneficial because it enables the manufacturer to create whatever thickness they want for conductive thread 208 (e.g., thick or thin) when covering the conductive core with the second layer.

[0067] After forming the conductive core, a cover layer is constructed to cover the conductive core. In one or more implementations, the cover layer is constructed by wrapping flexible threads (e.g., polyester threads, cotton threads, wool threads, or silk threads) around the conductive core. As an example, consider FIG. 4b which illustrates an example 404 of a conductive thread that includes a cover layer formed by wrapping flexible threads around a conductive core. In this example, conductive thread 208 is formed by wrapping flexible threads 308 around the conductive core (not pictured). For example, the cover layer may be formed by wrapping polyester threads around the conductive core at approximately 1900 turns per yard.

[0068] In one or more implementations, the cover layer includes flexible threads braided around the conductive core. The braided cover layer may be formed using the same type of braiding as described above with regards to FIG. 4a. Any type of flexible thread 308 may be used for the braided cover layer. The thickness of the flexible thread and the number of flexible threads that are braided around the conductive core can be selected based on the desired thickness of conductive thread 208. For example, if conductive thread 208 is intended to be used for denim, a thicker flexible thread (e.g., cotton) and/or a greater number of flexible threads may be used to form the cover layer.

[0069] In one or more implementations, conductive thread 208 is constructed with a “double-braided” structure. In this case, the conductive core is formed by braiding flexible threads, such as silk, with a conductive wire (e.g., copper), as described above. Then, the cover layer is formed by braiding flexible threads (e.g., silk, cotton, or polyester) around the braided conductive core. The double-braided structure is strong, and thus is unlikely to break when being pulled during the weaving process. For example, when the double-braided conductive thread is pulled, the braided structure contracts and forces the braided core of copper to contract also with

makes the whole structure stronger. Further, the double-braided structure is soft and looks like normal yarn, as opposed to a cable, which is important for aesthetics and feel.

[0070] Interactive textile 102 can be formed cheaply and efficiently, using any conventional weaving process (e.g., jacquard weaving or 3D-weaving), which involves interlacing a set of longer threads (called the warp) with a set of crossing threads (called the weft). Weaving may be implemented on a frame or machine known as a loom, of which there are a number of types. Thus, a loom can weave non-conductive threads 302 with conductive threads 208 to create interactive textile 102.

[0071] In example 300, conductive thread 208 is woven into interactive textile 102 to form a grid that includes a set of substantially parallel conductive threads 208 and a second set of substantially parallel conductive threads 208 that crosses the first set of conductive threads to form the grid. In this example, the first set of conductive threads 208 are oriented horizontally and the second set of conductive threads 208 are oriented vertically, such that the first set of conductive threads 208 are positioned substantially orthogonal to the second set of conductive threads 208. It is to be appreciated, however, that conductive threads 208 may be oriented such that crossing conductive threads 208 are not orthogonal to each other. For example, in some cases crossing conductive threads 208 may form a diamond-shaped grid. While conductive threads 208 are illustrated as being spaced out from each other in FIG. 3, it is to be noted that conductive threads 208 may be weaved very closely together. For example, in some cases two or three conductive threads may be weaved closely together in each direction.

[0072] Conductive wire 306 may be insulated to prevent direct contact between crossing conductive threads 208. To do so, conductive wire 306 may be coated with a material such as enamel or nylon. Alternately, rather than insulating conductive wire 306, interactive textile may be generated with three separate textile layers to ensure that crossing conductive threads 208 do not make direct contact with each other.

[0073] Consider, for example, FIG. 5 which illustrates an example 500 of an interactive textile 102 with multiple textile layers. In example 500, interactive textile 102 includes a first textile layer 502, a second textile layer 504, and a third textile layer 506. The three textile layers may be combined (e.g., by sewing or gluing the layers together) to form interactive textile 102. In this example, first textile layer 502 includes horizontal conductive threads 208, and second textile layer 504 includes vertical conductive threads 208. Third textile layer 506 does not include any conductive threads, and is positioned between first textile layer 502 and second textile layer 504 to prevent vertical conductive threads from making direct contact with horizontal conductive threads 208.

[0074] In one or more implementations, interactive textile 102 includes a top textile layer and a bottom textile layer. The top textile layer includes conductive threads 208 woven into the top textile layer, and the bottom textile layer also includes conductive threads woven into the bottom textile layer. When the top textile layer is combined with the bottom textile layer, the conductive threads from each layer form capacitive touch sensor 202.

[0075] Consider for example, FIG. 6 which illustrates an example 600 of a two-layer interactive textile 102 in accordance with one or more implementations. In this example, interactive textile 102 includes a first textile layer 602 and a

second textile layer 604. First textile layer 602 is considered the “top textile layer” and includes first conductive threads 606 woven into first textile layer 602. Second textile layer 604 is considered the “bottom textile layer” of interactive textile 102 and includes second conductive threads 608 woven into second textile layer 604. When integrated into flexible object 104, such as a clothing item, first textile layer 602 is visible and faces the user such that the user is able to interact with first textile layer 602, while second textile layer 604 is not visible. For instance, first textile layer 602 may be part of an “outside surface” of the clothing item, while second textile layer may be the “inside surface” of the clothing item.

[0076] When first textile layer 602 and second textile layer 604 are combined, first conductive threads 606 of first textile layer 602 couples to second conductive threads 608 of second textile layer 604 to form capacitive touch sensor 202, as described above. In one or more implementations, the direction of the conductive threads changes from first textile layer 602 to second textile layer 604 to form a grid of conductive threads, as described above. For example, first conductive threads 606 in first textile layer 602 may be positioned substantially orthogonal to second conductive threads 608 in second textile layer 604 to form the grid of conductive threads.

[0077] In some cases, first conductive threads 606 may be oriented substantially horizontally and second conductive threads 608 may be oriented substantially vertically. Alternately, first conductive threads 606 may be oriented substantially vertically and second conductive threads 608 may be oriented substantially horizontally. Alternately, first conductive threads 606 may be oriented such that crossing conductive threads 608 are not orthogonal to each other. For example, in some cases crossing conductive threads 606 and 608 may form a diamond-shaped grid.

[0078] First textile layer 602 and second textile layer 604 can be formed independently, or at different times. For example, a manufacturer may weave second conductive threads 608 into second textile layer 604. A designer could then purchase second textile layer 604 with the conductive threads already woven into the second textile layer 604, and create first textile layer 602 by weaving conductive thread into a textile design. First textile layer 602 can then be combined with second textile layer 604 to form interactive textile 102.

[0079] First textile layer and second textile layer may be combined in a variety of different ways, such as by weaving, sewing, or gluing the layers together to form interactive textile 102. In one or more implementations, first textile layer 602 and second textile layer 604 are combined using a jacquard weaving process or any type of 3D-weaving process. When first textile layer 602 and second textile layer 604 are combined, the first conductive threads 606 of first textile layer 602 couple to second conductive threads 608 of second textile layer 604 to form capacitive touch sensor 202, as described above.

[0080] In one or more implementations, second textile layer 604 implements a standard configuration or pattern of second conductive threads 608. Consider, for example, FIG. 7 which illustrates a more-detailed view 700 of second textile layer 604 of two-layer interactive textile 102 in accordance with one or more implementations. In this example, second textile layer 604 includes horizontal conductive threads 702 and vertical conductive threads 704 which intersect to form multiple grids 706 of conductive thread. It is to be noted,

however, that any standard configuration may be used, such as different sizes of grids or just lines without grids. The standard configuration of second conductive threads 608 in the second level enables a precise size, shape, and placement of interactive areas anywhere on interactive textile 102. In example 700, second textile layer 604 utilizes connectors 708 to form grids 706. Connectors 708 may be configured from a harder material, such as polyester.

[0081] Second conductive threads 608 of second textile layer 604 can be connected to electronic components of interactive textile 102, such as textile controller 204, output devices (e.g., an LED, display, or speaker), and so forth. For example, second conductive threads 608 of second textile layer 604 may be connected to electronic components, such as textile controller 204, using flexible PCB, creping, gluing with conductive glue, soldering, and so forth. Since second textile layer 604 is not visible, this enables coupling to the electronics in a way that the electronics and lines running to the electronics are not visible in the clothing item or soft object.

[0082] In one or more implementations, the pitch of second conductive threads 608 in second textile layer 604 is constant. As described herein, the “pitch” of the conductive threads refers to a width of the line spacing between conductive threads. Consider, for example, FIG. 8 which illustrates an additional example 800 of second textile layer 604 in accordance with one or more implementations. In this example, first textile layer 602 is illustrated as being folded back to reveal second textile layer 604. Horizontal conductive threads 802 and vertical conductive threads 804 are completely woven into second textile layer 604. As can be seen, the distance between each of the lines does not change, and thus the pitch is considered to be constant.

[0083] Alternately, in one or more implementations, the pitch of second conductive threads 608 in second textile layer 604 is not constant. The pitch can be varied in a variety of different ways. In one or more implementations, the pitch can be changed using shrinking materials, such as heat shrinking polymers. For example, the pitch can be changed by weaving polyester or heated yarn with the conductive threads of the second textile layer.

[0084] In one or more implementations second conductive threads 608 may be partially woven into the second textile layer 604. Then, the pitch of second conductive threads 608 can be changed by weaving first textile layer 602 with second textile layer 604. Consider, for example, FIG. 9 which illustrates an additional example 900 of a second textile layer 604 in accordance with one or more implementations. In this example, horizontal conductive threads 902 and vertical conductive threads 904 are only partially woven into second textile layer 604. The pitch of the horizontal and vertical conductive threads can then be altered by weaving first textile layer 602 with second textile layer 604.

[0085] During operation, capacitive touch sensor 202 may be configured to determine positions of touch-input on the grid of conductive thread 208 using self-capacitance sensing or projective capacitive sensing.

[0086] When configured as a self-capacitance sensor, textile controller 204 charges crossing conductive threads 208 (e.g., horizontal and vertical conductive threads) by applying a control signal (e.g., a sine signal) to each conductive thread 208. When an object, such as the user’s finger, touches the grid of conductive thread 208, the conductive threads 208 that

are touched are grounded, which changes the capacitance (e.g., increases or decreases the capacitance) on the touched conductive threads 208.

[0087] Textile controller 204 uses the change in capacitance to identify the presence of the object. To do so, textile controller 204 detects a position of the touch-input by detecting which horizontal conductive thread 208 is touched, and which vertical conductive thread 208 is touched by detecting changes in capacitance of each respective conductive thread 208. Textile controller 204 uses the intersection of the crossing conductive threads 208 that are touched to determine the position of the touch-input on capacitive touch sensor 202. For example, textile controller 204 can determine touch data by determining the position of each touch as X,Y coordinates on the grid of conductive thread 208.

[0088] When implemented as a self-capacitance sensor, “ghosting” may occur when multi-touch input is received. Consider, for example, that a user touches the grid of conductive thread 208 with two fingers. When this occurs, textile controller 204 determines X and Y coordinates for each of the two touches. However, textile controller 204 may be unable to determine how to match each X coordinate to its corresponding Y coordinate. For example, if a first touch has the coordinates X1, Y1 and a second touch has the coordinates X4, Y4, textile controller 204 may also detect “ghost” coordinates X1, Y4 and X4, Y1.

[0089] In one or more implementations, textile controller 204 is configured to detect “areas” of touch-input corresponding to two or more touch-input points on the grid of conductive thread 208. Conductive threads 208 may be woven closely together such that when an object touches the grid of conductive thread 208, the capacitance will be changed for multiple horizontal conductive threads 208 and/or multiple vertical conductive threads 208. For example, a single touch with a single finger may generate the coordinates X1, Y1 and X2, Y1. Thus, textile controller 204 may be configured to detect touch-input if the capacitance is changed for multiple horizontal conductive threads 208 and/or multiple vertical conductive threads 208. Note that this removes the effect of ghosting because textile controller 204 will not detect touch-input if two single-point touches are detected which are spaced apart.

[0090] Alternately, when implemented as a projective capacitance sensor, textile controller 204 charges a single set of conductive threads 208 (e.g., horizontal conductive threads 208) by applying a control signal (e.g., a sine signal) to the single set of conductive threads 208. Then, textile controller 204 senses changes in capacitance in the other set of conductive threads 208 (e.g., vertical conductive threads 208).

[0091] In this implementation, vertical conductive threads 208 are not charged and thus act as a virtual ground. However, when horizontal conductive threads 208 are charged, the horizontal conductive threads capacitively couple to vertical conductive threads 208. Thus, when an object, such as the user’s finger, touches the grid of conductive thread 208, the capacitance changes on the vertical conductive threads (e.g., increases or decreases). Textile controller 204 uses the change in capacitance on vertical conductive threads 208 to identify the presence of the object. To do so, textile controller 204 detects a position of the touch-input by scanning vertical conductive threads 208 to detect changes in capacitance. Textile controller 204 determines the position of the touch-input as the intersection point between the vertical conductive thread 208 with the changed capacitance, and the horizontal

conductive thread **208** on which the control signal was transmitted. For example, textile controller **204** can determine touch data by determining the position of each touch as X,Y coordinates on the grid of conductive thread **208**.

[0092] Whether implemented as a self-capacitance sensor or a projective capacitance sensor, capacitive sensor **208** is configured to communicate the touch data to gesture manager **218** to enable gesture manager **218** to determine gestures based on the touch data, which can be used to control object **104**, computing device **106**, or applications **216** at computing device **106**.

[0093] Gesture manager **218** can be implemented to recognize a variety of different types of gestures, such as touches, taps, swipes, holds, and covers made to interactive textile **102**. To recognize the various different types of gestures, gesture manager **218** is configured to determine a duration of the touch, swipe, or hold (e.g., one second or two seconds), a number of the touches, swipes, or holds (e.g., a single tap, a double tap, or a triple tap), a number of fingers of the touch, swipe, or hold (e.g., a one finger-touch or swipe, a two-finger touch or swipe, or a three-finger touch or swipe), a frequency of the touch, and a dynamic direction of a touch or swipe (e.g., up, down, left, right). With regards to holds, gesture manager **218** can also determine an area of capacitive touch sensor **202** of interactive textile **102** that is being held (e.g., top, bottom, left, right, or top and bottom). Thus, gesture manager **218** can recognize a variety of different types of holds, such as a cover, a cover and hold, a five finger hold, a five finger cover and hold, a three finger pinch and hold, and so forth.

[0094] FIG. **10A** illustrates an example **1000** of generating a control based on touch-input corresponding to a single-finger touch. In example **1000**, horizontal conductive threads **208** and vertical conductive threads **208** of capacitive touch sensor **202** form an X,Y grid. The X-axis in this grid is labeled X1, X2, X3, and X4, and the Y-axis is labeled Y1, Y2, and Y3. As described above, textile controller **204** can determine the location of each touch on this X,Y grid using self-capacitance sensing or projective capacitance sensing.

[0095] In this example, touch-input **1002** is received when a user touches interactive textile **102**. When touch-input **1002** is received, textile controller **204** determines the position and time of touch-input **1002** on the grid of conductive thread **208**, and generates touch data **1004** which includes the position of the touch: "X1,Y1", and a time of the touch: T0. Then, touch data **1004** is communicated to gesture manager **218** at computing device **106** (e.g., over network **108** via network interface **210**).

[0096] Gesture manager **218** receives touch data **1004**, and generates a gesture **1006** corresponding to touch data **1004**. In this example, gesture manager **218** determines gesture **1006** to be "single-finger touch" because the touch data corresponds to a single touch-input point (X1,Y1) at a single time period (T0). Gesture manager **218** may then initiate a control **1008** to activate a functionality of computing device **106** based on the single-finger touch gesture **1006** to control object **104**, computing device **106**, or an application **216** at computing device **106**. A single-finger touch gesture, for example, may be used to control computing device **106** to power-on or power-off, to control an application **216** to open or close, to control lights in the user's house to turn on or off, and so on.

[0097] FIG. **10B** illustrates an example **1000** of generating a control based on touch-input corresponding to a double-tap. In this example, touch-input **1010** and **1012** is received when

a user double taps interactive textile **102**, such as by quickly tapping interactive textile **102**. When touch-input **1010** and **1012** is received, textile controller **204** determines the positions and time of the touch-input on the grid of conductive thread **208**, and generates touch data **1014** which includes the position of the first touch: "X1,Y1", and a time of the first touch: T0. The touch data **1014** further includes the position of the second touch: "X1,Y1", and the time of the second touch: T1. Then, touch data **1014** is communicated to gesture manager **218** at computing device **106** (e.g., over network **108** via network interface **210**).

[0098] Gesture manager **218** receives touch data **1014**, and generates a gesture **1016** corresponding to the touch data. In this example, gesture manager **218** determines gesture **1016** as a "double-tap" based on two touches being received at substantially the same position at different times. Gesture manager **218** may then initiate a control **1018** to activate a functionality of computing device **106** based on the double-tap touch gesture **1016** to control object **104**, computing device **106**, or an application **216** at computing device **106**. A double-tap gesture, for example, may be used to control computing device **106** to power-on an integrated camera, start the play of music via a music application **216**, lock the user's house, and so on.

[0099] FIG. **10C** illustrates an example **1000** of generating a control based on touch-input corresponding to a two-finger touch. In this example, touch-input **1020** and **1022** is received when a user touches interactive textile **102** with two fingers at substantially the same time. When touch-input **1020** and **1022** is received, textile controller **204** determines the positions and time of the touch-input on the grid of conductive thread **208**, and generates touch data **1024** which includes the position of the touch by a first finger: "X1,Y1", at a time T0. Touch data **1024** further includes the position of the touch by a second finger: "X3,Y2", at the same time T0. Then, touch data **1024** is communicated to gesture manager **218** at computing device **106** (e.g., over network **108** via network interface **210**).

[0100] Gesture manager **218** receives touch data **1024**, and generates a gesture **1026** corresponding to the touch data. In this case, gesture manager **218** determines gesture **1026** as a "two-finger touch" based on two touches being received in different positions at substantially the same time. Gesture manager may then initiate a control **1028** to activate a functionality of computing device **106** based on two-finger touch gesture **1026** to control object **104**, computing device **106**, or an application **216** at computing device **106**. A two-finger touch gesture, for example, may be used to control computing device **106** to take a photo using an integrated camera, pause the playback of music via a music application **216**, turn on the security system at the user's house and so on.

[0101] FIG. **10D** which illustrates an example **1000** of generating a control based on touch-input corresponding to a single-finger swipe up. In this example, touch-input **1030**, **1032**, and **1034** is received when a user swipes upwards on interactive textile **102** using a single finger. When touch-input **1030**, **1032**, and **1034** is received, textile controller **204** determines the positions and time of the touch-input on the grid of conductive thread **208**, and generates touch data **1036** corresponding to the position of a first touch as "X1,Y1" at a time T0, a position of a second touch as "X1,Y2" at a time T1, and a position of a third touch as "X1,Y3" at a time T2. Then, touch data **1036** is communicated to gesture manager **218** at computing device **106** (e.g., over network **108** via network interface **210**).

[0102] Gesture manager 218 receives touch data 1036, and generates a gesture 1038 corresponding to the touch data. In this case, the gesture manager 218 determines gesture 1038 as a “swipe up” based on three touches being received in positions moving upwards on the grid of conductive thread 208. Gesture manager may then initiate a control 1040 to activate a functionality of computing device 106 based on the swipe up gesture 1038 to control object 104, computing device 106, or an application 216 at computing device 106. A swipe up gesture, for example, may be used to control computing device 106 to accept a phone call, increase the volume of music being played by a music application 216, or turn on lights in the user’s house.

[0103] While examples above describe, generally, various types of touch-input gestures that are recognizable by interactive textile 102, it is to be noted that virtually any type of touch-input gestures may be detected by interactive textile 102. For example, any type of single or multi-touch taps, touches, holds, swipes, and so forth, that can be detected by conventional touch-enabled smart phones and tablet devices, may also be detected by interactive textile 102.

[0104] In one or more implementations, gesture manager 218 enables the user to create gestures and assign the gestures to functionality of computing device 106. The created gestures may include taps, touches, swipes and holds as described above. In addition, gesture manager 218 can recognize gesture strokes, such as gesture strokes corresponding to symbols, letters, numbers, and so forth.

[0105] Consider, for example, FIG. 11 which illustrates an example 1100 of creating and assigning gestures to functionality of computing device 106 in accordance with one or more implementations.

[0106] In this example, at a first stage 1102, gesture manager 218 causes display of a record gesture user interface 1104 on a display of computing device 106 during a gesture mapping mode. The gesture mapping mode may be initiated by gesture manager 218 automatically when interactive textile 102 is paired with computing device 106, or responsive to a control or command initiated by the user to create and assign gestures to functionalities of computing device 106.

[0107] In the gesture mapping mode, gesture manager 218 prompts the user to input a gesture to interactive textile 102. Textile controller 204, at interactive textile 102, monitors for gesture input to interactive textile 102 woven into an item of clothing (e.g., a jacket) worn by the user, and generates touch data based on the gesture. The touch data is then communicated to gesture manager 218.

[0108] In response to receiving the touch data from interactive textile 102, gesture manager 218 analyzes the touch data to identify the gesture. Gesture manager 218 may then cause display of a visual representation 1106 of the gesture on display 220 of computing device 106. In this example, visual representation 1106 of the gesture is a “v” which corresponds to the gesture that is input to interactive textile 102. Gesture user interface includes a next control 1108 which enables the user to transition to a second stage 1110.

[0109] At second stage 1110, gesture manager 218 enables the user to assign the gesture created at first stage 1102 to a functionality of computing device 106. As described herein, a “functionality” of computing device 106 can include any command, control, or action at computing device 102. Examples of functionalities of computing device 106 may include, by way of example and not limitation, answering a

call, music playing controls (e.g., next song, previous song, pause, and play), requesting the current weather, and so forth.

[0110] In this example, gesture manager 218 causes display of an assign function user interface 1112 which enables the user to assign the gesture created at first stage 1102 to one or more functionalities of computing device 102. Assign function user interface 1112 includes a list 1114 of functionalities that are selectable by the user to assign or map the gesture to the selected functionality. In this example, list 1114 of functionalities includes “refuse call”, “accept call”, “play music”, “call home”, and “silence call”.

[0111] Gesture manager receives user input to assign function user interface 1112 to assign the gesture to a functionality, and assigns the gesture to the selected functionality. In this example, the user selects the “accept call” functionality, and gesture manager 218 assigns the “v” gesture created at first stage 1102 to the accept call functionality.

[0112] Assigning the created gesture to the functionality of computing device 106 enables the user to initiate the functionality, at a subsequent time, by inputting the gesture into interactive textile 102. In this example, the user can now make the “v” gesture on interactive textile 102 in order to cause computing device 106 to accept a call to computing device 106.

[0113] Gesture manager 218 is configured to maintain mappings between created gestures and functionalities of computing device 106 in a gesture library. The mappings can be created by the user, as described above. Alternately or additionally, the gesture library can include predefined mappings between gestures and functionalities of computing device 106.

[0114] As an example, consider FIG. 12 which illustrates an example 1200 of a gesture library in accordance with one or more implementations. In example 1200, the gesture library includes multiple different mappings between gestures and device functionalities of computing device 106. At 1202, a “circle” gesture is mapped to a “tell me the weather” function, at 1204 a “v” gesture is mapped to an accept call function, at 1206 an “x” gesture is mapped to a “refuse call” function, at 1208 a “triangle” gesture is mapped to a “call home” function, at 1210 an “m” gesture is mapped to a “play music” function, and at 1212 a “w” gesture is mapped to a “silence call” function.

[0115] As noted above, the mappings at 1202, 1204, 1206, 1208, 1210, and 1212 may be created by the user or may be predefined such that the user does not need to first create and assign the gesture. Further, the user may be able to change or modify the mappings by selecting the mapping and creating a new gesture to replace the currently assigned gesture.

[0116] Notably, there may be a variety of different functionalities that the user may wish to initiate via a gesture to interactive textile 102. However, there is a limited number of different gestures that a user can realistically be expected to remember. Thus, in one or more implementations gesture manager 218 is configured to select a functionality based on both a gesture to interactive textile 102 and a context of computing device 106. The ability to recognize gestures based on context enables the user to invoke a variety of different functionalities using a subset of gestures. For example, for a first context, a first gesture may initiate a first functionality, whereas for a second context, the same first gesture may initiate a second functionality.

[0117] In some cases, the context of computing device 106 may be based on an application that is currently running on

computing device **106**. For example, the context may correspond to listening to music when the user is utilizing a music player application to listen to music, and to “receiving a call” when a call is communicated to computing device **106**. In these cases, gesture manager **218** can determine the context by determining the application that is currently running on computing device **106**.

[0118] Alternately or additionally, the context may correspond to an activity that the user is currently engaged in, such as running, working out, driving a car, and so forth. In these cases, gesture manager **218** can determine the context based on sensor data received from sensors implemented at computing device **106**, interactive textile **102**, or another device that is communicably coupled to computing device **106**. For example, acceleration data from an accelerometer may indicate that the user is currently running, driving in a car, riding a bike, and so forth. Other non-limiting examples of determining context include determining the context based on calendar data (e.g., determining the user is in a meeting based on the user’s calendar), determining context based on location data, and so forth.

[0119] After the context is determined, textile controller **204**, at interactive textile **102**, monitors for gesture input to interactive textile **102** woven into an item of clothing (e.g., a jacket) worn by the user, and generates touch data based on the gesture input. The touch data is then communicated to gesture manager **218**.

[0120] In response to receiving the touch data from interactive textile **102**, gesture manager **218** analyzes the touch data to identify the gesture. Then, gesture manager **218** initiates a functionality of computing device based on the gesture and the context. For example, gesture manager **218** can compare the gesture to a mapping that assigns gestures to different contexts. A given gesture, for example, may be associated with multiple different contexts and associated functionalities. Thus, when a first gesture is received, gesture manager **218** may initiate a first functionality if a first context is detected, or initiate a second, different functionality if a second, different context is detected.

[0121] As an example, consider FIG. **13** which illustrates an example **1300** of contextual-based gestures to an interactive textile in accordance with one or more implementations.

[0122] In this example, computing device **106** is implemented as a smart phone **1302** that is communicably coupled to interactive textile **102**. For example, interactive textile **102** may be woven into a jacket worn by the user, and coupled to smart phone **1302** via a wireless connection such as Bluetooth.

[0123] At **1304**, smart phone **1302** is in a “music playing” context because a music player application is playing music on smart phone **1302**. In the music playing context, gesture manager **218** has assigned a first subset of functionalities to a first subset of gestures at **1306**. For example, the user can play a previous song by swiping left on interactive textile **102**, play or pause a current song by tapping interactive textile **102**, or play a next song by swiping right on interactive textile **102**.

[0124] At **1308**, the context of smart phone **1302** changes to an “incoming call” context when smart phone **1302** receives an incoming call. In the incoming call context, the same subset of gestures is assigned to a second subset of functionalities which are associated with the incoming call context at **1310**. For example, by swiping left on interactive textile **102** the user can now reject the call, whereas before swiping left would have caused the previous song to be played in the

music playing context. Similarly, by tapping interactive textile **102** the user can accept the call, and by swiping right on interactive textile **102** the user can silence the call.

[0125] In one or more implementations, interactive textile **102** further includes one or more output devices, such as one or more light sources (e.g., LED’s), displays, speakers, and so forth. These output devices can be configured to provide feedback to the user based on touch-input to interactive textile **102** and/or notifications based on control signals received from computing device **106**.

[0126] FIG. **14** which illustrates an example **1400** of a jacket that includes an interactive textile **102** and an output device in accordance with one or more implementations. In this example, interactive textile **102** is integrated into the sleeve of a jacket **1402**, and is coupled to a light source **1404**, such as an LED, that is integrated into the cuff of jacket **1402**.

[0127] Light source **1404** is configured to output light, and can be controlled by textile controller **204**. For example, textile controller **204** can control a color and/or a frequency of the light output by light source **1404** in order to provide feedback to the user or to indicate a variety of different notifications. For example, textile controller **204** can cause the light source to flash at a certain frequency to indicate a particular notification associated with computing device **106**, e.g., a phone call is being received, a text message or email message has been received, a timer has expired, and so forth. Additionally, textile controller **204** can cause the light source to flash with a particular color of light to provide feedback to the user that a particular gesture or input to interactive textile **102** has been recognized and/or that an associated functionality is activated based on the gesture.

[0128] FIG. **15** illustrates implementation examples **1500** of interacting with an interactive textile and an output device in accordance with one or more implementations.

[0129] At **1502**, textile controller **204** causes a light source to flash at a specific frequency to indicate a notification that is received from computing device **106**, such as an incoming call or a text message.

[0130] At **1504**, the user places his hand over interactive textile **102** to cover the interactive textile. This “cover” gesture may be mapped to a variety of different functionalities. For example, this gesture may be used to silence a call or to accept a call. In response, the light source can be controlled to provide feedback that the gesture is recognized, such as by turning off when the call is silenced.

[0131] At **1506**, the user taps the touch sensor with a single finger to initiate a different functionality. For example, the user may be able to place one finger on the touch sensor to listen to a voicemail on computing device **106**. In this case, the light source can be controlled to provide feedback that the gesture is recognized, such as by outputting orange light when the voicemail begins to play.

[0132] Having discussed interactive textiles **102**, and how interactive textiles **102** detect touch-input, consider now a discussion of how interactive textiles **102** may be easily integrated within flexible objects **104**, such as clothing, handbags, fabric casings, hats, and so forth.

[0133] FIG. **16** illustrates various examples **1600** of interactive textiles integrated within flexible objects. Examples **1600** depict interactive textile **102** integrated in a hat **1602**, a shirt **1604**, and a handbag **1606**.

[0134] Interactive textile **102** is integrated within the bill of hat **1602** to enable the user to control various computing devices **106** by touching the bill of the user’s hat. For

example, the user may be able to tap the bill of hat **1602** with a single finger at the position of interactive textile **102**, to answer an incoming call to the user's smart phone, and to touch and hold the bill of hat **1602** with two fingers to end the call.

[0135] Interactive textile **102** is integrated within the sleeve of shirt **1604** to enable the user to control various computing devices **106** by touching the sleeve of the user's shirt. For example, the user may be able to swipe to the left or to the right on the sleeve of shirt **1604** at the position of interactive textile **102** to play a previous or next song, respectively, on a stereo system of the user's house.

[0136] In examples **1602** and **1604**, the grid of conductive thread **208** is depicted as being visible on the bill of the hat **1602** and on the sleeve of shirt **1604**. It is to be noted, however, that interactive textile **102** may be manufactured to be the same texture and color as object **104** so that interactive textile **102** is not noticeable on the object.

[0137] In some implementations, a patch of interactive textile **102** may be integrated within flexible objects **104** by sewing or gluing the patch of interactive textile **102** to flexible object **104**. For example, a patch of interactive textile **102** may be attached to the bill of hat **1602**, or to the sleeve of shirt **1604** by sewing or gluing the patch of interactive textile **102**, which includes the grid of conductive thread **208**, directly onto the bill of hat **1602** or the sleeve of shirt **1604**, respectively. Interactive textile **102** may then be coupled to textile controller **204** and power source **206**, as described above, to enable interactive textile **102** to sense touch-input.

[0138] In other implementations, conductive thread **208** of interactive textile **102** may be woven into flexible object **104** during the manufacturing of flexible object **104**. For example, conductive thread **208** of interactive textile **102** may be woven with non-conductive threads on the bill of hat **1602** or the sleeve of a shirt **1604** during the manufacturing of hat **1602** or shirt **1604**, respectively.

[0139] In one or more implementations, interactive textile **102** may be integrated with an image on flexible object **104**. Different areas of the image may then be mapped to different areas of capacitive touch sensor **202** to enable a user to initiate different controls for computing device **106**, or application **216** at computing device **106**, by touching the different areas of the image. In FIG. **16**, for example, interactive textile **102** is weaved with an image of a flower **1608** onto handbag **1606** using a weaving process such as jacquard weaving. The image of flower **1608** may provide visual guidance to the user such that the user knows where to touch the handbag in order to initiate various controls. For example, one petal of flower **1608** could be used to turn on and off the user's smart phone, another petal of flower **1608** could be used to cause the user's smart phone to ring to enable the user to find the smart phone when it is lost, and another petal of flower **1608** could be mapped to the user's car to enable the user to lock and unlock the car.

[0140] Similarly, in one or more implementations interactive textile **102** may be integrated with a three-dimensional object on flexible object **104**. Different areas of the three-dimensional object may be mapped to different areas of capacitive touch sensor **202** to enable a user to initiate different controls for computing device **106**, or application **216** at computing device **106**, by touching the different areas of the three-dimensional object. For example, bumps or ridges can be created using a material such as velvet or corduroy and woven with interactive textile **102** onto object **104**. In this

way, the three-dimensional objects may provide visual and tactile guidance to the user to enable the user to initiate specific controls. A patch of interactive textile **102** may be weaved to form a variety of different 3D geometric shapes other than a square, such as a circle, a triangle, and so forth.

[0141] In various implementations, interactive textile **102** may be integrated within a hard object **104** using injection molding. Injection molding is a common process used to manufacture parts, and is ideal for producing high volumes of the same object. For example, injection molding may be used to create many things such as wire spools, packaging, bottle caps, automotive dashboards, pocket combs, some musical instruments (and parts of them), one-piece chairs and small tables, storage containers, mechanical parts (including gears), and most other plastic products available today.

Example Methods

[0142] FIGS. **17**, **18**, **19**, and **20** illustrate an example method **1700** (FIG. **17**) of generating touch data using an interactive textile, an example method **1800** (FIG. **18**) of determining gestures usable to initiate functionality of a computing device, an example method **1900** (FIG. **19**) of assigning a gesture to a functionality of a computing device, and an example method **2000** (FIG. **20**) of initiating a functionality of a computing device based on a gesture and a context. These methods and other methods herein are shown as sets of blocks that specify operations performed but are not necessarily limited to the order or combinations shown for performing the operations by the respective blocks. In portions of the following discussion reference may be made to environment **100** of FIG. **1** and system **200** of FIG. **2**, reference to which is made for example only. The techniques are not limited to performance by one entity or multiple entities operating on one device.

[0143] FIG. **17** illustrates an example method **1700** of generating touch data using an interactive textile.

[0144] At **1702**, touch-input to a grid of conductive thread woven into an interactive textile is detected. For example, textile controller **204** (FIG. **2**) detects touch-input to the grid of conductive thread **208** woven into interactive textile **102** (FIG. **1**) when an object, such as a user's finger, touches interactive textile **102**.

[0145] Interactive textile **102** may be integrated within a flexible object, such as shirt **104-1**, hat **104-2**, or handbag **104-3**. Alternately, interactive textile **102** may be integrated with a hard object, such as plastic cup **104-4** or smart phone casing **104-5**.

[0146] At **1704**, touch data is generated based on the touch-input. For example, textile controller **204** generates touch data based on the touch-input. The touch data may include a position of the touch-input on the grid of conductive thread **208**.

[0147] As described throughout, the grid of conductive thread **208** may include horizontal conductive threads **208** and vertical conductive threads **208** positioned substantially orthogonal to the horizontal conductive threads. To detect the position of the touch-input, textile controller **204** can use self-capacitance sensing or projective capacitance sensing.

[0148] At **1706**, the touch data is communicated to a computing device to control the computing device or one or more applications at the computing device. For example, network interface **210** at object **104** communicates the touch data generated by textile controller **204** to gesture manager **218** implemented at computing device **106**. Gesture manager **218**

and computing device **106** may be implemented at object **104**, in which case interface may communicate the touch data to gesture manager **218** via a wired connection. Alternately, gesture manager **218** and computing device **106** may be implemented remote from interactive textile **102**, in which case network interface **210** may communicate the touch data to gesture manager **218** via network **108**.

[0149] FIG. **18** illustrates an example method **1800** of determining gestures usable to initiate functionality of a computing device in accordance with one or more implementations.

[0150] At **1802**, touch data is received from an interactive textile. For example, network interface **222** (FIG. **2**) at computing device **106** receives touch data from network interface **210** at interactive textile **102** that is communicated to gesture manager **218** at step **906** of FIG. **9**.

[0151] At **1804**, a gesture is determined based on the touch data. For example, gesture manager **218** determines a gesture based on the touch data, such as single-finger touch gesture **506**, a double-tap gesture **516**, a two-finger touch gesture **526**, a swipe gesture **538**, and so forth.

[0152] At **1806**, a functionality is initiated based on the gesture. For example, gesture manager **218** generates a control based on the gesture to control an object **104**, computing device **106**, or an application **216** at computing device **106**. For example, a swipe up gesture may be used to increase the volume on a television, turn on lights in the user's house, open the automatic garage door of the user's house, and so on.

[0153] FIG. **19** illustrates an example method **1900** of assigning a gesture to a functionality of a computing device in accordance with one or more implementations.

[0154] At **1902**, touch data is received at a computing device from an interactive textile woven into an item of clothing worn by the user. For example, network interface **222** (FIG. **2**) at computing device **106** receives touch data from network interface **210** at interactive textile **102** that is woven into an item of clothing worn by a user, such as a jacket, shirt, hat, and so forth.

[0155] At **1904**, the touch data is analyzed to identify a gesture. For example, gesture manager **218** analyzes the touch data to identify a gesture, such as a touch, tap, swipe, hold, or gesture stroke.

[0156] At **1906**, user input to assign the gesture to a functionality of the computing device is received. For example, gesture manager **218** receives user input to assign function user interface **1112** to assign the gesture created at step **1904** to a functionality of computing device **106**.

[0157] At **1908**, the gesture is assigned to the functionality of the computing device. For example, gesture manager **218** assigns the functionality selected at step **1906** to the gesture created at step **1904**.

[0158] FIG. **20** illustrates an example method **2000** of initiating a functionality of a computing device based on a gesture and a context in accordance with one or more implementations.

[0159] At **2002**, a context associated with a computing device or a user of the computing device is determined. For example, gesture manager **218** determines a context associated with computing device **106** or a user of computing device **106**.

[0160] At **2004**, touch data is received at the computing device from an interactive textile woven into a clothing item worn by the user. For example, touch data is received at

computing device **106** from interactive textile **102** woven into a clothing item worn by the user, such as jacket, shirt, or hat.

[0161] At **2006**, the touch data is analyzed to identify a gesture. For example, gesture manager **218** analyzes the touch data to identify a gesture, such as a touch, tap, swipe, hold, stroke, and so forth.

[0162] At **2008**, a functionality is activated based on the gesture and the context. For example, gesture manager **218** activates a functionality based on the gesture identified at step **2006** and the context determined at step **2002**.

[0163] The preceding discussion describes methods relating to gestures for interactive textiles. Aspects of these methods may be implemented in hardware (e.g., fixed logic circuitry), firmware, software, manual processing, or any combination thereof. These techniques may be embodied on one or more of the entities shown in FIGS. **1-16** and **21** (computing system **2100** is described in FIG. **21** below), which may be further divided, combined, and so on. Thus, these figures illustrate some of the many possible systems or apparatuses capable of employing the described techniques. The entities of these figures generally represent software, firmware, hardware, whole devices or networks, or a combination thereof.

Example Computing System

[0164] FIG. **21** illustrates various components of an example computing system **2100** that can be implemented as any type of client, server, and/or computing device as described with reference to the previous FIGS. **1-20** to implement two-layer interactive textiles. In embodiments, computing system **2100** can be implemented as one or a combination of a wired and/or wireless wearable device, System-on-Chip (SoC), and/or as another type of device or portion thereof. Computing system **2100** may also be associated with a user (e.g., a person) and/or an entity that operates the device such that a device describes logical devices that include users, software, firmware, and/or a combination of devices.

[0165] Computing system **2100** includes communication devices **2102** that enable wired and/or wireless communication of device data **2104** (e.g., received data, data that is being received, data scheduled for broadcast, data packets of the data, etc.). Device data **2104** or other device content can include configuration settings of the device, media content stored on the device, and/or information associated with a user of the device. Media content stored on computing system **2100** can include any type of audio, video, and/or image data. Computing system **2100** includes one or more data inputs **2106** via which any type of data, media content, and/or inputs can be received, such as human utterances, touch data generated by interactive textile **102**, user-selectable inputs (explicit or implicit), messages, music, television media content, recorded video content, and any other type of audio, video, and/or image data received from any content and/or data source.

[0166] Computing system **2100** also includes communication interfaces **2108**, which can be implemented as any one or more of a serial and/or parallel interface, a wireless interface, any type of network interface, a modem, and as any other type of communication interface. Communication interfaces **2108** provide a connection and/or communication links between computing system **2100** and a communication network by which other electronic, computing, and communication devices communicate data with computing system **2100**.

[0167] Computing system 2100 includes one or more processors 2110 (e.g., any of microprocessors, controllers, and the like), which process various computer-executable instructions to control the operation of computing system 2100 and to enable techniques for, or in which can be embodied, interactive textiles. Alternatively or in addition, computing system 2100 can be implemented with any one or combination of hardware, firmware, or fixed logic circuitry that is implemented in connection with processing and control circuits which are generally identified at 2112. Although not shown, computing system 2100 can include a system bus or data transfer system that couples the various components within the device. A system bus can include any one or combination of different bus structures, such as a memory bus or memory controller, a peripheral bus, a universal serial bus, and/or a processor or local bus that utilizes any of a variety of bus architectures.

[0168] Computing system 2100 also includes computer-readable media 2114, such as one or more memory devices that enable persistent and/or non-transitory data storage (i.e., in contrast to mere signal transmission), examples of which include random access memory (RAM), non-volatile memory (e.g., any one or more of a read-only memory (ROM), flash memory, EPROM, EEPROM, etc.), and a disk storage device. A disk storage device may be implemented as any type of magnetic or optical storage device, such as a hard disk drive, a recordable and/or rewritable compact disc (CD), any type of a digital versatile disc (DVD), and the like. Computing system 2100 can also include a mass storage media device 2116.

[0169] Computer-readable media 2114 provides data storage mechanisms to store device data 2104, as well as various device applications 2118 and any other types of information and/or data related to operational aspects of computing system 2100. For example, an operating system 2120 can be maintained as a computer application with computer-readable media 2114 and executed on processors 2110. Device applications 2118 may include a device manager, such as any form of a control application, software application, signal-processing and control module, code that is native to a particular device, a hardware abstraction layer for a particular device, and so on.

[0170] Device applications 2118 also include any system components, engines, or managers to implement interactive textiles. In this example, device applications 2118 include gesture manager 218.

CONCLUSION

[0171] Although embodiments of techniques using, and objects including, two-layer interactive textiles have been described in language specific to features and/or methods, it is to be understood that the subject of the appended claims is not necessarily limited to the specific features or methods described. Rather, the specific features and methods are disclosed as example implementations of two-layer interactive textiles.

What is claimed is:

1. An interactive textile configured to be integrated within a flexible object, the interactive textile comprising:
 - a top textile layer comprising first conductive threads woven into the top textile layer;
 - a bottom textile layer comprising second conductive threads woven into the bottom textile layer, the first

conductive threads and the second conductive threads configured to form a capacitive touch sensor; and
 a textile controller coupled to the capacitive touch sensor, the textile controller configured to detect touch-input to the capacitive touch sensor when an object touches the capacitive touch sensor, and process the touch-input to provide touch data usable to control a computing device wirelessly coupled to the interactive textile.

2. The interactive textile as recited in claim 1, wherein the textile controller is coupled to the capacitive touch sensor via the second conductive threads of the bottom textile layer.

3. The interactive textile as recited in claim 1, wherein the first conductive threads woven into the top textile layer and the second conductive threads woven into the bottom textile layer form a grid of conductive threads.

4. The interactive textile as recited in claim 3, wherein the first conductive threads woven into the top textile layer are positioned substantially orthogonal to the second conductive threads woven into the second textile layer to form the grid of conductive threads.

5. The interactive textile as recited in claim 1, wherein a pitch of the second conductive threads woven into the second textile layer is constant.

6. The interactive textile as recited in claim 1, wherein a pitch of the second conductive threads woven into the second textile layer is not constant.

7. The interactive textile as recited in claim 6, wherein shrinking polymers are used to vary the pitch of the second conductive threads woven into the second textile layer.

8. The interactive textile as recited in claim 6, wherein the second conductive threads are partially woven into the second textile layer.

9. The interactive textile as recited in claim 1, wherein the first textile layer and the second textile layer are combined using a 3D-weaving process.

10. The interactive textile as recited in claim 1, wherein the flexible object comprises a clothing item.

11. The interactive textile as recited in claim 10, wherein the first textile layer comprises an outside surface of the clothing item.

12. The interactive textile as recited in claim 1, wherein the second textile layer comprises a standardized structure of second conductive threads.

13. The interactive textile as recited in claim 1, wherein the first and second conductive threads each comprise a conductive wire that is twisted, wrapped, or braided with one or more flexible threads.

14. The interactive textile as recited in claim 13, wherein the conductive wire comprises a copper wire, a gold wire, or a silver wire.

15. A flexible object comprising:
 - an interactive textile integrated within the flexible object, the interactive textile comprising a top textile layer and a bottom textile layer, the top textile layer comprising first conductive threads woven into the top textile layer and the bottom textile layer comprising second conductive threads woven into the bottom textile layer; and
 - a textile controller coupled to the interactive textile, the textile controller configured to detect touch-input to the interactive textile, and process the touch-input to provide touch data usable to initiate functionality of a computing device wireless coupled to the interactive textile.

16. The flexible object as recited in claim 15, wherein the textile controller is coupled to the interactive textile via the second conductive threads of the bottom textile layer.

17. The flexible object as recited in claim 15, wherein the flexible object comprises a clothing item.

18. The flexible object as recited in claim 15, wherein the second conductive threads and the textile controller are not visible when the clothing item is worn by a user.

19. The flexible object as recited in claim 15, wherein a pitch of the second conductive threads woven into the second textile layer is constant.

20. The flexible object as recited in claim 15, wherein the first textile layer and the second textile layer are combined using a 3D-weaving process.

* * * * *

Inside The Design Of Google's First Smart Jacket

Google's futuristic Project Jacquard is making its commercial debut—as a jean jacket.

JOHN BROWNLEE 05.23.16 1:00 PM

Last year, Google announced Project Jacquard: an intriguing plan to turn all of your clothes into touchscreen controllers, partnering with Levi's to incorporate the technology into its denim products.

Now, a year later, and Levi's and Google have announced the first retail garment with Project Jacquard inside: the Levi's Commuter x Jacquard, a trucker jacket with a multitouch sleeve that lets you control your Android smartphone—without ever pulling it out of your pocket.



WHY A JACKET?

During an ATAP presentation at Google I/O on Friday, interaction designer Ivan Poupyrev and Levi's VP of Innovation, Paul Dillinger, took the stage to show off what the Commuter x Jacquard could do. The jacket has a patch on the sleeve that serves as the interface between you and your phone. It's aimed primarily at bike commuters; a cyclist riding down the street could tap the sleeve of their jacket to get an ETA on how long it will take for them to reach work, swipe the cuff to cycle songs on Spotify, double tap to accept an incoming call, or triple tap to dismiss it.

Last year when I spoke to Poupyrev and Dillinger about the Jacquard-Levi's partnership, both spoke in loose terms about what they intended to do—except to say that Google had chosen Levi's as an initial partner for Jacquard because "if you can make Jacquard work with denim, you can do it with anything." This is because denim goes through a notoriously tortuous manufacturing process, which involves the material being literally blasted with fire at one stage. So the first question I asked them this year was why they decided to make a jacket—instead of a pair of jeans or some other product.

There aren't many garments that we find personally or socially acceptable to wear more than half of our waking lives without changing.

The decision to make a jacket, says Dillinger, ultimately came from a desire to make a garment which was useful all the time. "How many jeans do you have in your closet, compared to how many jackets?" he asks. "In our research, we discovered that 70% of our customers have at least one jacket they wear more than three days a week." He points out that there aren't many garments that we find personally or socially acceptable to wear more than half of our waking lives without changing.

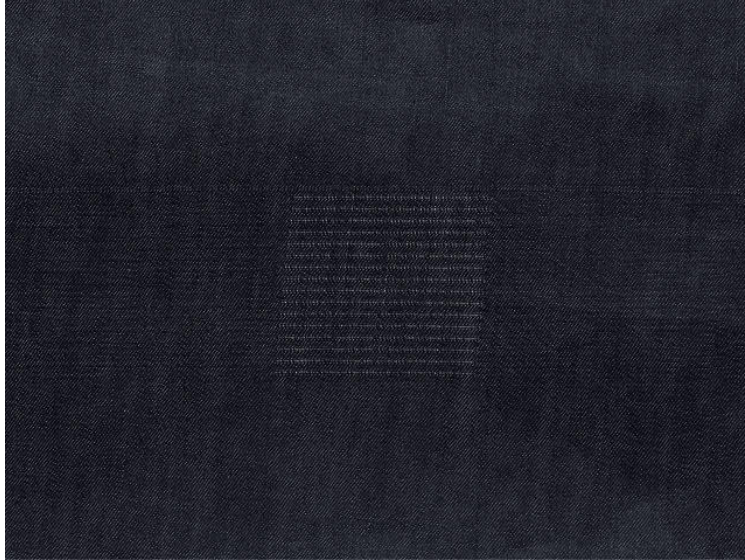
DEVELOPING UX STANDARDS FOR FASHION

So in appearance, the Levi's Commuter x Jacquard is a fairly standard denim trucker jacket, with Project Jacquard woven into the wrist. The controller, which connects via Bluetooth to your smartphone, is a flexible rubber dongle. But it doesn't look like one: it looks like a cuff. It connects to the Project Jacquard patch by snapping on like a button near the sleeve, then wrapping around the cuff, like the fabric loop attached to the buttons on the cuff of a classic trench coat. "We wanted the controller to function within the existing vocabulary of fashion," Dillinger tells me. The controller plugs into a standard USB port to juice, and can go days without a charge.

Another way in which Jacquard has been adapted to fit within the existing vocabulary of denim is the way the touch panel is woven into the garment. Poupyrev says that one of the UX problems they've wrestled with in Jacquard is how visible to make the touch panel. Make it too prominent, and it distracts from the integrity of a garment; make it invisible, and users don't know where to touch. In the case of the jacket, Levi's and Google came up with a beautiful compromise that makes the Jacquard panel visible but is still authentic to the way denim is made. In denim manufacturing, there's a natural weaving flaw called a missed pick in the weft, which represents itself as a visible seam in the material: a dark line, representing a literal gap where a line of thread is missing in the piece of cloth. It's totally natural, and since it's a problem that mostly happens on denim that is hand woven on older machines, missed picks are strongly associated with vintage denim.

Instead of looking high-tech, the Jacquard patch on the jacket looks charmingly imperfect, and desirably bespoke.

With the Commuter jacket, Levi's integrated Jacquard by weaving the conductive threads of the technology into a grid of purposely missed weft picks. So, instead of looking high-tech, the Jacquard patch on the jacket looks charmingly imperfect, and desirably bespoke. "I'm just amazed at the poetry of that solution," says Poupyrev. By introducing this weaving error on purpose, Levi's gave the Commuter jacket an authenticity amongst denim lovers that it might otherwise have lacked.



Eventually, says Poupyrev, Google wants to find ways to work with other garment makers to integrate Jacquard into products. "The whole point of Jacquard is to work within the confines of existing production techniques to make fabric smarter," he says. "So the trick for every kind of material is to find an implementation of Jacquard that does not feel like an imposition upon [each fabric or garment] maker's craft." So whether Jacquard comes to men's suits, silk scarves, Victoria's Secret bras, or high-tech Speedos next, it needs to do so in a way that feels authentic to the material.

In the meantime, Project Jacquard will be exclusive to the Levi's Commuter x Jacquard. It will launch in beta in autumn this year, and start shipping in 2017—at a price that Levi's says shouldn't prompt consumers used to purchasing high-performance denim jackets to run screaming for the hills.

All Images: courtesy Levi's Commuter x Jacquard

<http://www.fastcodesign.com/3060133/inside-the-design-of-googles-first-smart-jacket>

Here's Why Google and Levi's Are Working Together to Make a Jean Jacket

The leaders of Google's Project Jacquard and Levi's product innovation discuss why they think a jean jacket will make you covet smart clothes.

by [Rachel Metz](#)

May 26, 2016

[Ivan Poupyrev](#) and [Paul Dillinger](#) come from very different worlds: Poupyrev, a technical program lead for Google's Advanced Technologies and Projects (ATAP) unit, has spent years working on user-interface design and interactive technology, while Dillinger, the head of global product innovation for Levi Strauss & Co., has immersed himself in fashion.

These worlds collided more than a year ago, though, when Levi's agreed to work with Google on [Project Jacquard](#), an interactive fabric project that Poupyrev heads. It aims to create conductive textiles that can be manufactured like regular fabrics and woven into everything from shirts to teddy bears. The idea is that you'll then be able to [swipe and tap](#) the fabric to do things like control music or get directions.

Right now, Poupyrev and Dillinger are gearing up to roll out the first Jacquard-enabled consumer product that will do these things in 2017: a jean jacket aimed at cycling commuters with conductive thread woven into one arm that connects to a removable, flexible electronic tag (the tag comes off so you can charge its battery and wash the jacket).



Poupyrev and Dillinger spoke with *MIT Technology Review* last week about how they decided on what to bring to market first, the difficulties of building interactivity into different kinds of fabrics, and when we might see a Project Jacquard couch.

How did you decide to make a jacket as the first consumer product for Project Jacquard? And what was that design process like?

Dillinger: When we started talking to consumers we found there's a big group of people that had one jacket that was their go-to functional jacket that they would wear like three times a week or more. And they wore it that often because it had some utility, value. We wanted this thing to have value, we wanted people to use it often, and the best place to get that frequent use was going to be a piece of outerwear.



Paul Dillinger, Levi's head of global product innovation, is working with Project Jacquard to create a smart jacket that you can swipe and tap to do things like control music.

There are also certain technical constraints. You launder your jackets less frequently than you launder your [jeans]. This was before we had all the confidence about the washability, this was when we were anticipating having to be a little more careful with it—what's that one garment that isn't going to go in the washing machine as often?

[And making] a commuter jacket made the needs even more explicit. When you're on your bike, it's about safety, awareness, focus. And that need started to inform the function that we saw as a potential value of this integrated woven tactile interface.

Lots of people have been working on smart fabrics, smart clothing for years. Nobody has been able to make it mainstream. Why do you think Google can do this with Project Jacquard?

Poupyrev: Instead of trying to take something from Levi's and add our something as an add-on and sell it, we're actually trying to integrate our technology into the supply chain, the manufacturing chain of the garment industry. So we don't want to make our own garments. That was the biggest decision made by our team, by me, pretty much, from the very beginning, these

fundamental things: we will not make our garments, we will empower industry to make their garments. And the industry is gigantic.

Dillinger: Where there's a chance for success here where there hadn't been in the past has to do with the configuration of the decision-making process. The people inventing the technology are not the people saying yes to using the technology. In this case, the invention of the technology was done by Google ... and it was up to us to say, "That we can do it doesn't mean that we should do it."

What are some big differences between how textiles are made versus consumer electronics that Google has had to adjust to?



Ivan Poupyrev, leader of Google's Project Jacquard, is trying to make smart fabric that can be easily manufactured.

Poupyrev: The supply chain and delivery of the goods is completely different. The way we think about shipping is completely different. In the consumer electronics industry, everything is identical. Here, you take different samples of denim—the color, weave, structure are slightly different.

The factory that's making the conductive yarn is also a little different from what you'd typically encounter in consumer electronics, right?

Poupyrev: There's a small factory that's been there for 50 years in the mountains of Japan. The guy [who runs it], he's like 80 years old. He doesn't know how to use e-mail. He doesn't know how to use a mobile phone. He refuses to accept any phone calls. He only uses fax.

I don't remember [the output of yarn] exactly but it's something like a meter every second or maybe every two seconds they're able to produce. If you look at the [consumer electronics] production line, you have a phone coming out every two seconds from the production line. And we have, like, a piece of yarn. Like, alright, we're talking about different scales here.

What are some major remaining issues for making interactive fabrics producible and usable on a mass scale?

Poupyrev: I think the big issue right now is we resolved this for cotton. The reality is that the variety of fabrics out there is just incredible, and all of them have a different manufacturing process. Not only different manufacturing processes, but the factories that provide them are specialized. The factory that makes denim only makes denim, a cotton-based fabric. They don't do silk, they don't do polyester, they don't do synthetic fabrics ... they don't do wool, they don't do, like, fine organza stuff. That's a completely different factory. Now we think, "Okay, how are we going to scale that into wool, how are we going to scale that into synthetic fibers which are used by companies like Patagonia or North Face?"

Beyond clothing, lots of things rely on fabric—like chairs and toys, for instance. Where else might Jacquard fabric show up over the next year or two?

Poupyrev: Textiles is one of those materials that's ubiquitous. So absolutely, we want to go further, we want to expand, we look at this as a platform. But we need to focus. We need to start with something and I think clothing and apparel is exciting. People get excited about it, people love it. There's a lot of clothing being made. Fashion is awesome. We think we need to get it solved for the garment. If we solve for the garment, we can solve for the couches and for the cars and for the airplanes and seats or whatever textiles.

Vogue Meets Levi's Historian, Tracey Panek

vogue.co.uk/news/2016/07/25/tracey-panek-levis-historian-interview

25 July 2016

Katie Berrington

Ahead of [Levi's](#) inclusion in the [V&A's](#) *You Say You Want a Revolution? Rebels & Records 1966 - 1970* exhibition this autumn, *Vogue* meets the brand's historian, Tracey Panek, to talk about Levi's historical influence, her favourite archive items and the stories behind some of the brand's most iconic pieces.

Tracey Panek

Picture credit: Twitter/TraceyPanek

What's it been like to work with the V&A?

It's really exciting! The V&A is one of my favorite museums and it's been a real pleasure working with them. I toured their conservation area earlier this week and was struck by the similarities. At the Levi Strauss & Co. archives in San Francisco, we even use the same type of boxes to store our and conserve our vintage garments as the V&A.



I think one of the things that sets this partnership apart is how authentic it feels for both partners. The Sixties were not only a defining moment in popular culture but also a period when LS&Co. was at the forefront of the generational and social zeitgeist. One of the V&A's curators came to visit us in San Francisco last year and, together, we picked Levi's pieces that could best showcase the themes in the exhibition, which was great. We'll be featuring a pair of our iconic 501 jeans, a Fifties leather jacket (the ultimate "rebel wear" piece) and an amazing pair of customised 505 jeans. The colours on the 505 from the patches and embellishments will really knock people out. We're also including a pair of bellbottoms and Super Slim jeans from our Orange Tab line that was first introduced in 1969.

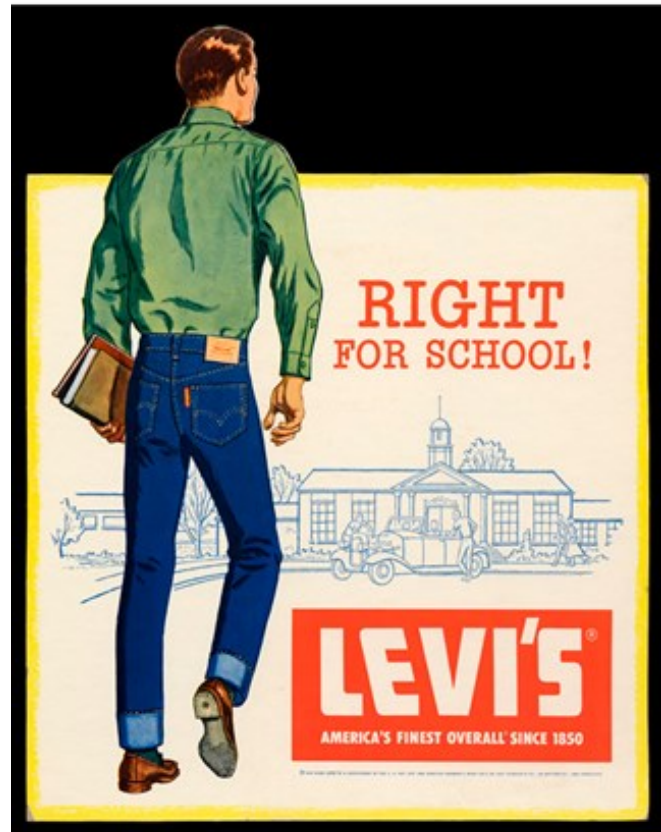
What defines that period - the late Sixties - in fashion to you?

Fashion can be a key indicator of time and culture. The late Sixties and early Seventies were an explosive time, symbolised by a rising youth culture experimenting with music, drugs, counter-culture ideals and political activism. These happenings influenced fashion, with dress becoming a personal expression of one's philosophies and individuality. Colour, customisation and thrift-shop chic were among the distinctive elements of style and blue jeans and denim became a canvas for such personal expression.

The introduction of Levi's 505 jeans in 1967 fit seamlessly into this era and was quickly adopted by many teenagers, hippies and rock-and-rollers. A classic straight leg jean in pre-shrunk denim with a zipper, rather than a button fly, the slim-fitting 505 became the unofficial uniform for many trailblazers and musicians who came to define the era. From rockers like the Rolling Stones who used the jeans' zipper fly on the cover of *Sticky Fingers* to punk bands like the Ramones, the "coming of age" 505 jean became a staple for later rock stars like Debbie Harry.

What influence do you think Levi's had on that era and vice versa?

The association of Levi's jeans with youth culture, music and individual style flourished in the Sixties. The late Sixties and early Seventies were an incredibly rich cultural period - where youth led a change in the social-political-cultural zeitgeist. Peace marches, the desire for sexual freedom, student protests and an explosion of music left a lasting influence on today's society, with Levi's interwoven into the fabric of that time. With our headquarters set in San Francisco, an epicenter of that cultural change, Levi's garments naturally became integrated into the social fabric of the era.



Do you own any vintage pieces from that era that you love?

I've been a life-long fan of Levi's jeans and wore 501 jeans throughout high school. The 501 was the world's first blue jean and the blueprint for all jeans today. They are a classic and were a must-have item for my three sisters and I during school. I wished I had saved those jeans when I left home for college!

What's your personal favourite period of time in terms of fashion and why?

I'm a product of fashion in the Eighties when I was in high school. I wore shrink-to-fit Levi's 501s and borrowed a skinny black silk tie from my dad - something he wore in the Fifties. The tie reminds me of one I saw at the Rock and Roll Hall of Fame owned by Buddy Holly. He wore it with a black suit and it's typical of the time. My 501s, dad's tie and a red pullover sweater was a favorite outfit from that time. I was just starting to develop my own sense of style back then.



Can you tell us more about your role as the Levi Strauss historian?

I feel incredibly fortunate that I'm able to apply my passion for history at work every day. As the historian for Levi Strauss & Co., I work closely with executives, employees and the public to understand, interpret and share the heritage of the brand. I also manage the archives and work closely with our design team studying historic items from the collection to use as inspiration for future products. On top of that, I'm always on the lookout for new additions to the archives and am regularly searching and asking questions to gain a deeper understanding of how LS&Co. fits into larger scope of history.

What elements of the role do you particularly enjoy?

I love hearing stories from Levi's fans! The stories range from one of a man I met in Moscow whose father bought Levi's jeans on the black market during the Cold War and a woman in India who just starting wearing our women's 711 skinny jean, to the story of Barbara, an 80-plus-year-old woman from Los Angeles who found our famous Calico 1890 waist overalls in a mine in the Mojave Desert as a teenager in the Forties.

What, in your opinion, is the most interesting/surprising thing about the history of the brand?

I've been pleasantly surprised by the interconnections of the Levi's brand with key cultural moments in history. This happened to me while I was visiting London. I learned that a Levi Strauss & Co. leather jacket worn by Albert Einstein was going to be up for auction. I went to Christie's Auction House to see it and ended being the successful bidder.

Einstein bought the jacket sometime in the mid-Thirties when he was preparing for naturalisation - a fitting symbol of his journey to becoming an "official American" by purchasing an iconic American brand. Einstein was famously photographed in the Levi's jacket throughout the period and appeared in it on the cover of *Time* magazine in 1938.

In a surprising coming together of Einstein and the Levi's brand, *Time* magazine named Einstein Man of the Century in 1999 when his photo was again featured on the cover. In the same issue, Levi's 501 jeans were named the Fashion Item of the 20th Century.



What are your favourite items from the archive?

I'm naturally drawn to the oldest pieces in the collection and especially those with an interesting story. The 1890 Calico waist overalls, the early name for blue jeans, is a favourite. I met [Barbara] who found the pants as a teenager. Today, in her eighties, she's still a spunky woman. She wore the found jeans to high school until she discovered how old they were from a pocket bag inscription and donated them to LS&Co.

Along with Calico, my favourites list continues to grow. The Einstein jacket is definitely going on that list. It still retains the scent of Einstein's pipe smoke!

You Say You Want a Revolution? Rebels & Records 1966 - 1970 opens at the V&A on September 10.



US009624608B2

(12) **United States Patent**
Martin et al.

(10) **Patent No.:** **US 9,624,608 B2**
(45) **Date of Patent:** **Apr. 18, 2017**

(54) **ARCHITECTURALLY REINFORCED DENIM**

(71) Applicants: **John F. Martin**, Beaverton, OR (US);
LaShurya M. Wise, Portland, OR (US)

(72) Inventors: **John F. Martin**, Beaverton, OR (US);
LaShurya M. Wise, Portland, OR (US)

(73) Assignee: **NIKE, Inc.**, Beaverton, OR (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 791 days.

(21) Appl. No.: **13/767,505**

(22) Filed: **Feb. 14, 2013**

(65) **Prior Publication Data**

US 2013/0217288 A1 Aug. 22, 2013

Related U.S. Application Data

(60) Provisional application No. 61/600,286, filed on Feb. 17, 2012.

(51) **Int. Cl.**

D03D 13/00 (2006.01)
D03D 15/00 (2006.01)
B32B 5/06 (2006.01)
D03D 15/08 (2006.01)
D03D 1/00 (2006.01)
A41D 31/00 (2006.01)

(52) **U.S. Cl.**

CPC **D03D 13/004** (2013.01); **B32B 5/06** (2013.01); **D03D 13/00** (2013.01); **D03D 15/08** (2013.01); **A41D 31/0055** (2013.01); **D03D 1/0035** (2013.01); **D10B 2201/02** (2013.01); **D10B 2331/021** (2013.01); **D10B 2401/02** (2013.01); **D10B 2401/063** (2013.01); **D10B 2501/04** (2013.01); **Y10T 442/3179** (2015.04)

(58) **Field of Classification Search**

CPC .. D03D 1/0041; D03D 15/00; A41D 31/0011;
D02G 3/02; D02G 3/04; D02G 3/047;
D02G 3/442

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,077,126 A * 12/1991 Green D02G 3/442
428/373
5,837,623 A 11/1998 Howland
5,918,319 A * 7/1999 Baxter A41D 1/067
2/22

(Continued)

FOREIGN PATENT DOCUMENTS

CN 102227524 A 6/2008
CN 201074263 Y 6/2008

(Continued)

OTHER PUBLICATIONS

International Search Report and Written Opinion of May 20, 2013 for PCT/US13/26700.

(Continued)

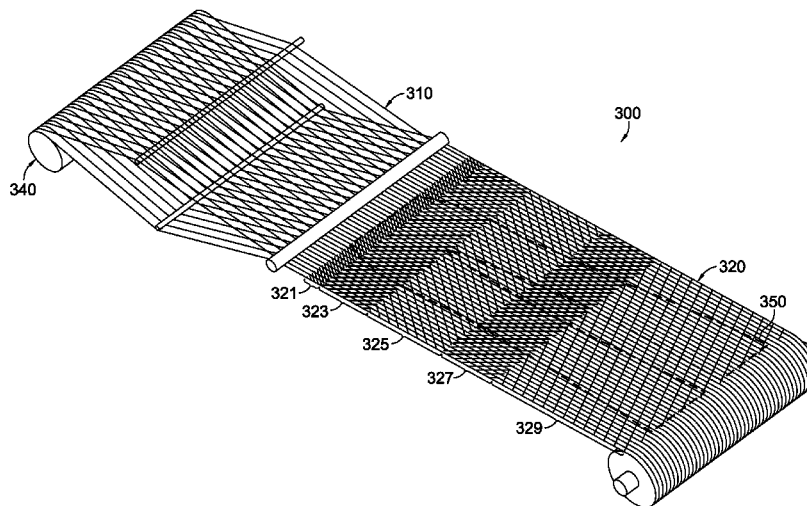
Primary Examiner — Jenna Johnson

(74) *Attorney, Agent, or Firm* — Shook, Hardy & Bacon L.L.P.

(57) **ABSTRACT**

A denim fabric with high tenacity and/or moisture management and/or stretch materials is provided. Proportions of materials in the denim fabric may vary during the weave of the fabric to create different performance zones in the resulting garment with or without assembling different fabric pieces.

16 Claims, 5 Drawing Sheets



US 9,624,608 B2

Page 2

(56)

References Cited

U.S. PATENT DOCUMENTS

6,666,235 B2 12/2003 Chi
6,668,868 B2 12/2003 Howland
7,062,789 B1* 6/2006 Blackwell A41D 1/08
2/79
7,156,883 B2 1/2007 Lovasic
7,214,425 B2 5/2007 Kolmes
7,820,565 B2 10/2010 Van Heerden
2002/0106956 A1 8/2002 Howland
2002/0111099 A1 8/2002 Howland
2003/0066571 A1 4/2003 Ono
2005/0081939 A1 4/2005 Heiman
2005/0208855 A1 9/2005 Zhu
2005/0255776 A1 11/2005 Howland
2007/0136930 A1 6/2007 Dipietro
2007/0243783 A1 10/2007 Kotani
2007/0249250 A1 10/2007 Servajejan
2008/0229484 A1 9/2008 Baychar
2010/0075557 A1* 3/2010 Shteyer D03D 1/0041
442/203

2010/0325766 A1* 12/2010 Mackintosh A41D 13/00
2/22
2011/0000020 A1 1/2011 Walvius
2011/0070412 A1* 3/2011 Ly B32B 5/10
428/196
2011/0300366 A1 12/2011 Henssen

FOREIGN PATENT DOCUMENTS

CN 201459336 U 5/2010
DE 102005045151 A1 3/2007
JP 201037683 A 2/2010
WO 2010079989 A2 7/2010
WO 2011034683 A1 3/2011
WO 2011137213 A2 11/2011
WO WO 2012016124 A2* 2/2012 D03D 15/00

OTHER PUBLICATIONS

European Supplementary Search Report dated Jul. 7, 2015 in
Application No. 13749348.2, 6 pages.

* cited by examiner

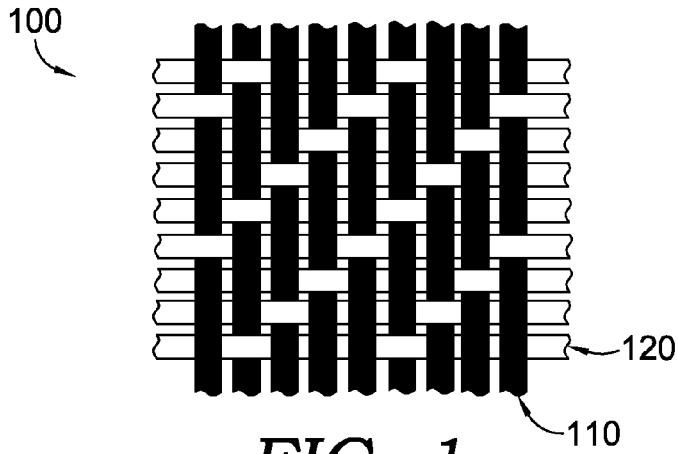


FIG. 1.

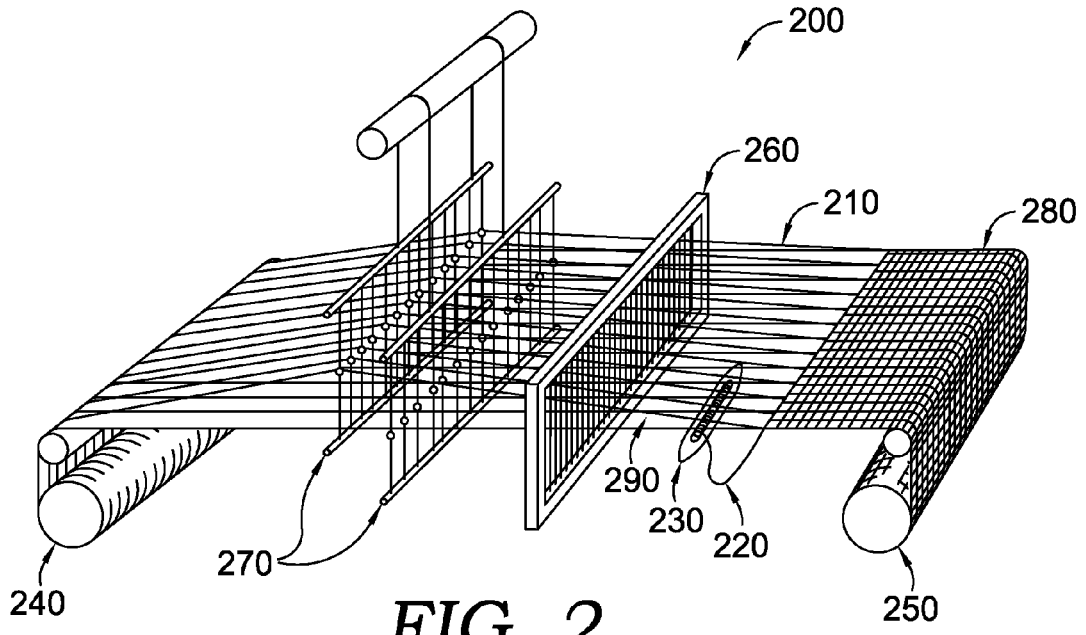


FIG. 2.

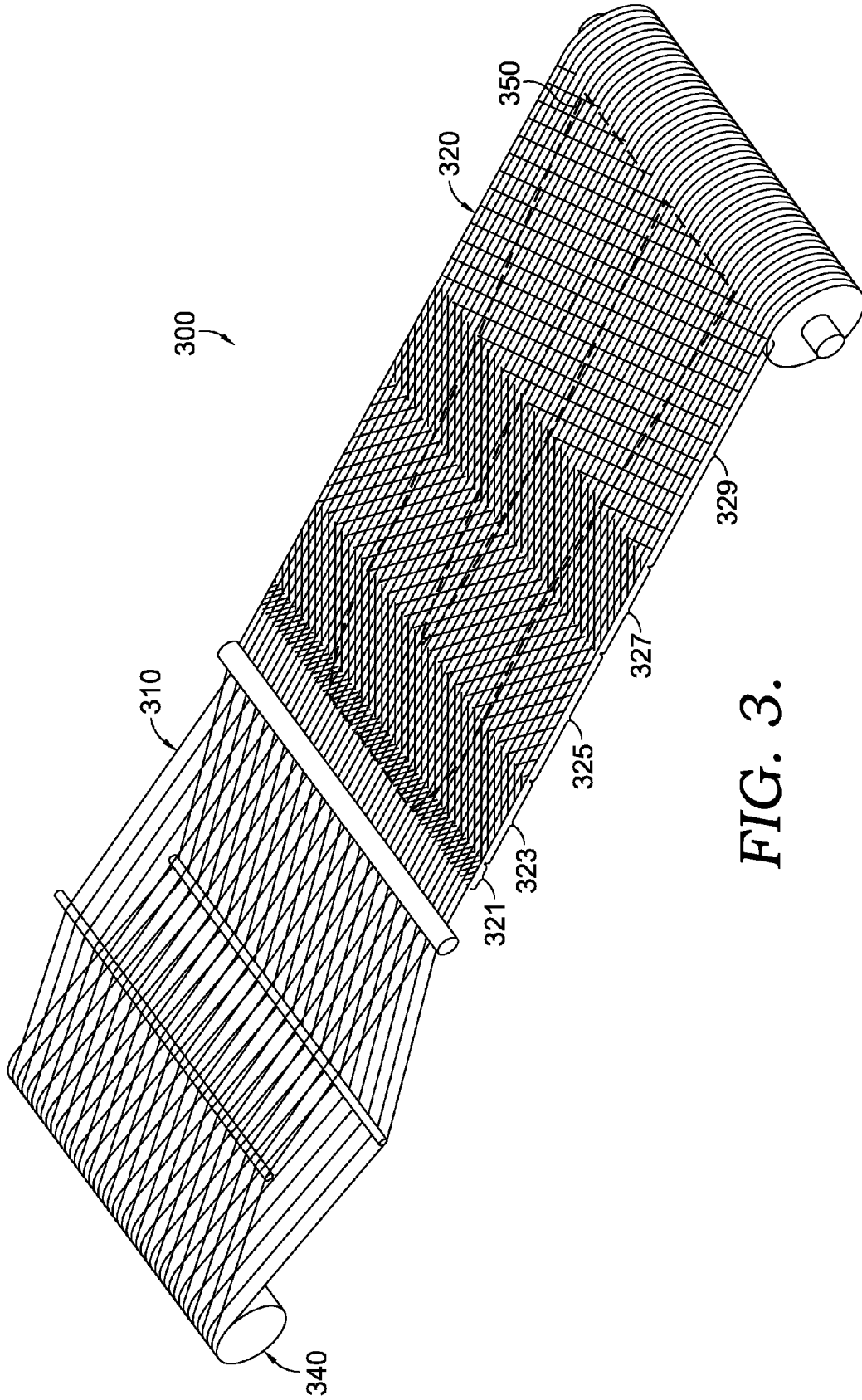


FIG. 3.

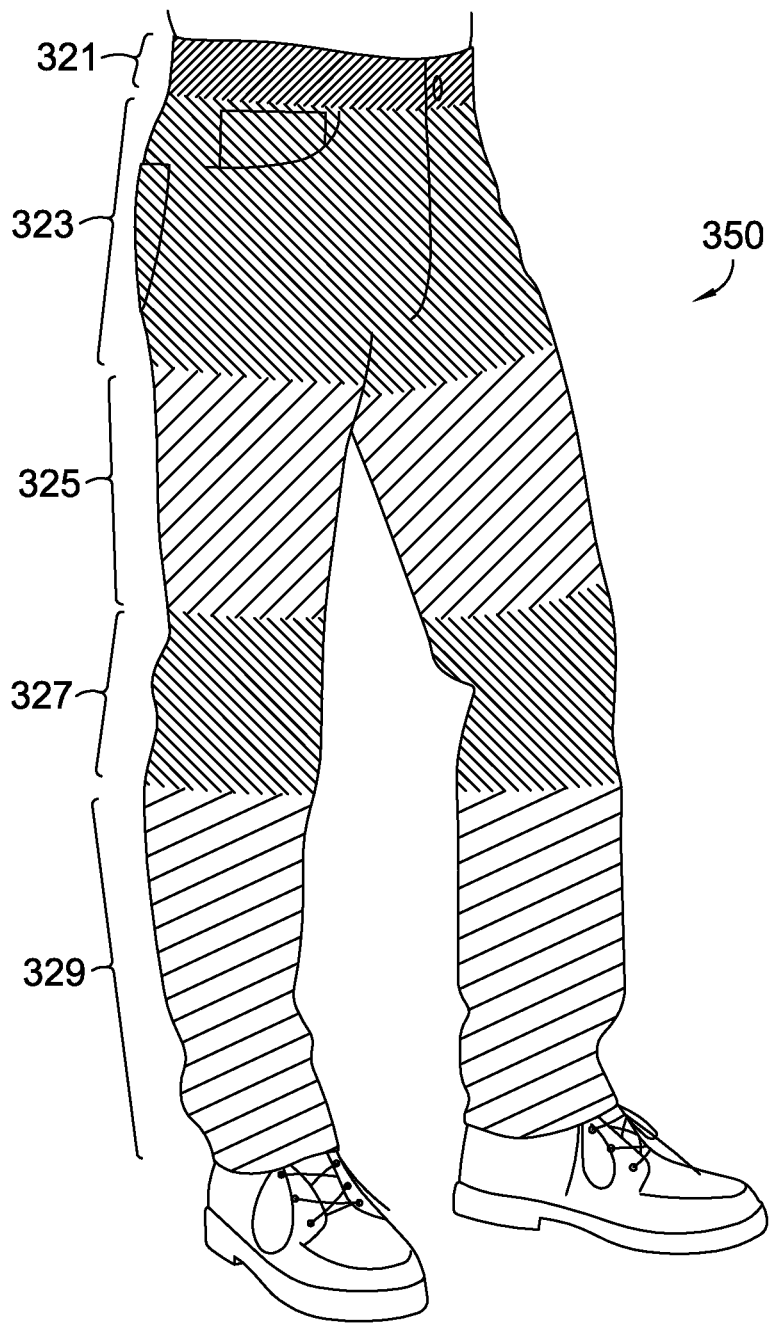


FIG. 4.

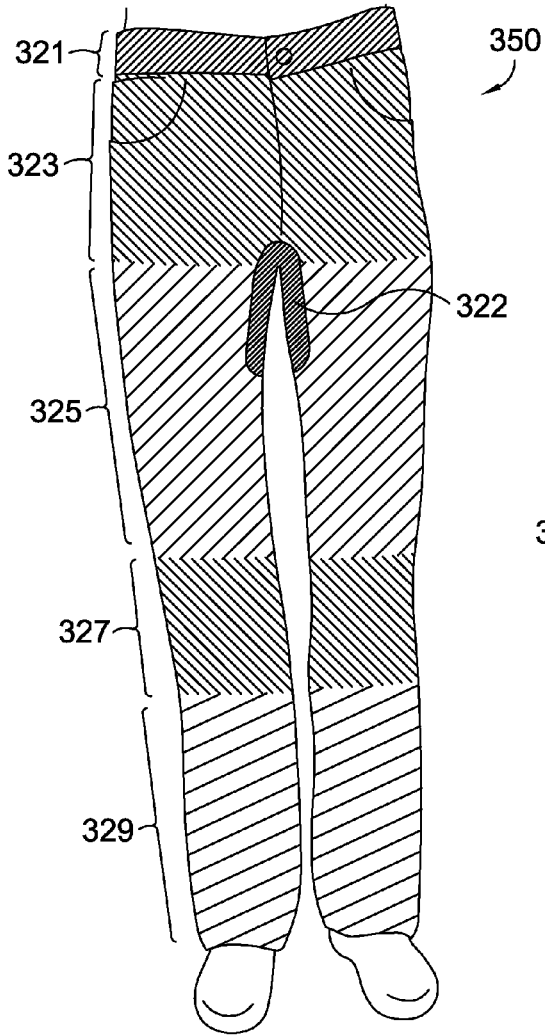


FIG. 5A.

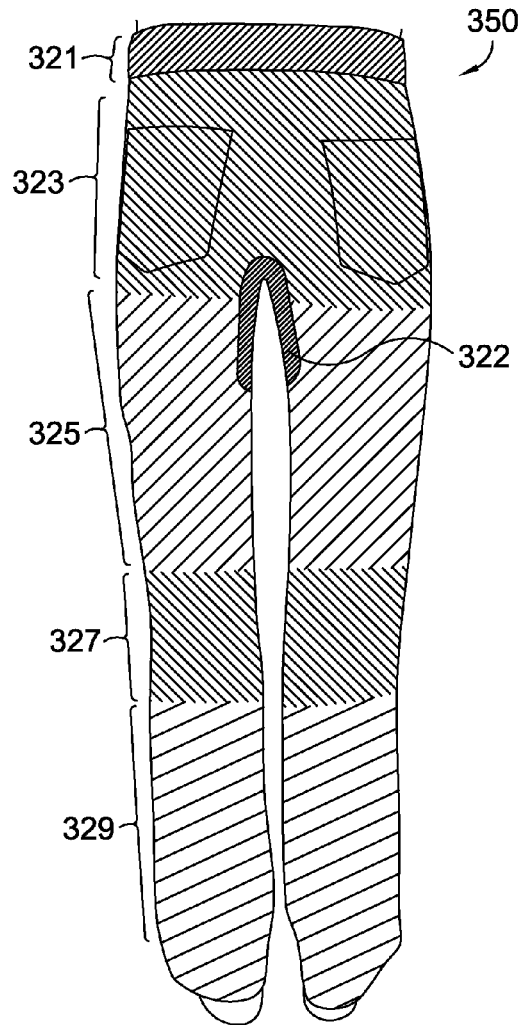


FIG. 5B.

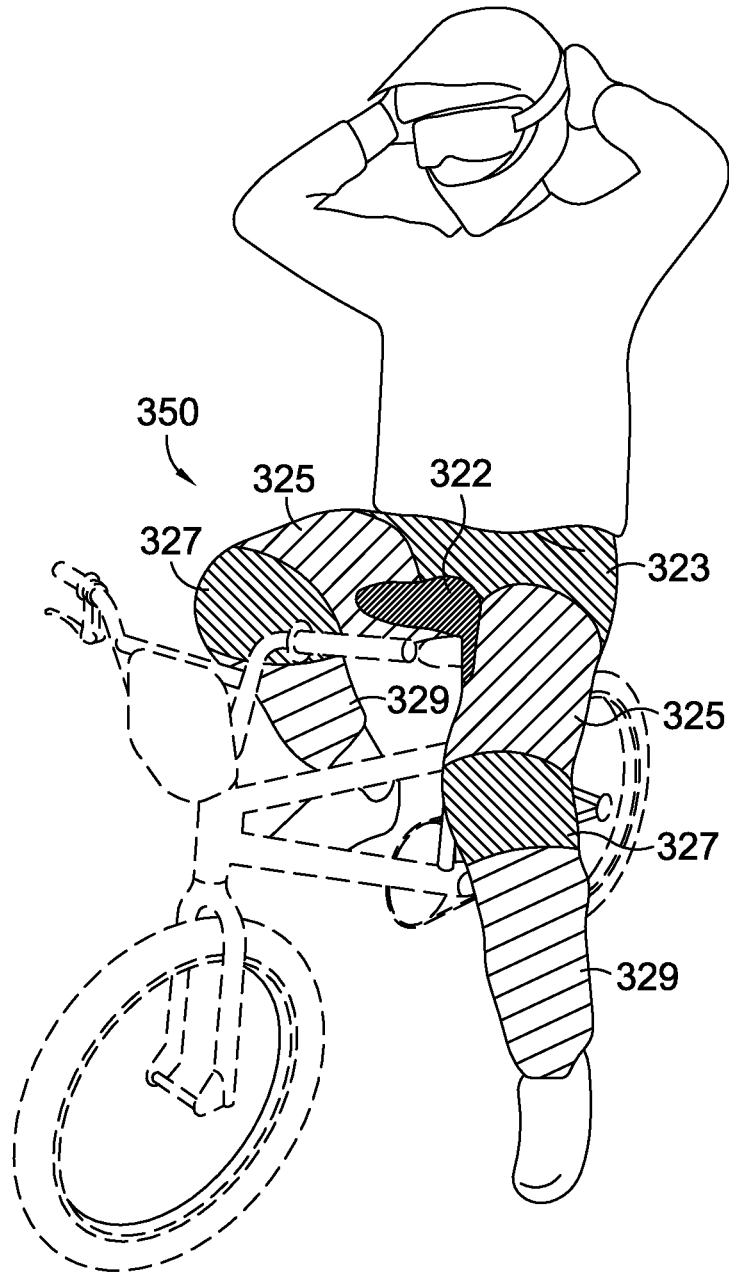


FIG. 5C.

1

ARCHITECTURALLY REINFORCED DENIM**CROSS-REFERENCE TO RELATED APPLICATIONS**

This application claims the benefit of U.S. Provisional Application No. 61/600,286, filed Feb. 17, 2012, entitled "Architecturally Reinforced Denim," which is incorporated in its entirety by reference herein.

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

Not applicable.

TECHNICAL FIELD

The present invention relates to architecturally reinforced denim fabrics. In particular, the present invention relates to architecturally reinforced denim fabrics for the use in manufacturing athletic gear for athlete of extreme sports, having moisture regulation properties and high structural integrity, even after repeated exposure to external environmental elements such as friction against cement, rock, metal, or dirt, particularly when the athlete is engaged in the particular sport.

BACKGROUND OF THE INVENTION

Athletes who practice extreme sports such as FMX, BMX, adventure racing, skateboarding, sandboarding, and many others, require specialized gear that must be comfortable and protective, but these athletes also prefer clothing and other gear that are fashionable and attractive. The specialized gear needs to be able to withstand the great physical exertion of the athlete and the exposure to different external elements that result from the environment of the particular sport.

For decades now, denim has been a popular "American comfort" staple in everyone's closet, both in the United States and around the world. While denim is a relatively tough and durable fabric, conventional denim lacks the resilience and other performance and/or comfort characteristics desired for athletic endeavors particularly extreme sports. It is an object of this invention to provide a denim fabric and gear made from this fabric suitable for extreme sports athletes, providing them with comfort and an outstanding level of protection, while being fashionable and attractive.

SUMMARY OF THE INVENTION

This summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used as an aid in determining the scope of the claimed subject matter.

The present invention relates to an architecturally reinforced denim fabric and articles of manufacture made from this architecturally reinforced denim fabric. One example of the architecturally reinforced denim fabric of the present invention may be light weight and may possess moisture management properties facilitating the wicking of moisture from the wearer's skin. Denim in accordance with the present invention may provide elasticity that adds comfort and flexibility.

2

Denim fabric in accordance with the present invention may incorporate commercially available strengthening polymer fibers that are abrasion, temperature and/or chemical resistant. Examples of such fibers are available under such trade names as Kevlar (available from DuPont), Vectran® (available from Kuraray Co., Ltd.), Dyneema® (available from DSM Dyneema), Gold Flex® (available from Honeywell), Twanron® (available from AKZO), Nomex® (available from DuPont), and any other polymer fiber with similar physicochemical properties. These strengthening polymer fibers, when combined with cotton fibers, may yield lightweight durable denim fabrics with puncture and tear resistance while still maintaining comfort.

Yet in another example of the present invention, the architecturally reinforced denim fabric of the present invention may incorporate both moisture wicking fibers and strengthening polymer fibers in combination with cotton fibers. This denim fabric with moisture management properties and strengthening fibers may provide comfort when in contact with the skin of the wearer while still providing protection for the wearer.

The denim fabric of the present invention may be used to manufacture bottoms such as pants, shorts, skirts, tops such as jackets, shirts, etc. Other items of apparel such as hats, gloves, etc., may be manufactured in accordance with the present invention. The denim fabric of the present invention may also be used in the fabrication of shoes or shoe parts, such as shoe uppers.

The denim of the present invention may be different tones of the typical indigo blue, or may also be different tones of other colors such as black, red, orange, yellow, pink, purple, green, or any other color available for the dyeing of cotton based fabrics, or any combination of colors and tones of the dyes.

Any style of pants may be constructed in accordance with the present invention. Examples of pants for male athletes of extreme sports of the present invention may be skinny, slim, straight, baggy, taper, boot cut, or classic fits such as relaxed or comfort fit jeans, or jeans with any other custom fit chosen to be appropriate for the particular sport. Examples of pants for female athletes of extreme sports of the present invention may be leggings, slim, skinny, boot cut, flare, baggy, wide leg fit jeans, or jeans with any other custom fit chosen to be appropriate for the particular sport. The pants manufactured from the denim fabric of the present invention may incorporate padding in areas of high impact, such as the buttocks and the knees, to offer impact absorption in case of a fall.

In a further example, pants may be manufactured utilizing a combination components made of classic 100% cotton denim and components made of one or more denim fabrics in accordance with the present invention. In another example, pants may be manufactured from a combination of different denim fabrics of the present invention, such as moisture management denim and strengthened denim, or moisture management denim and strengthened denim with added moisture management capabilities, etc. Different types of denim may be combined to create a single garment in accordance with the present invention by stitching or otherwise joining together different types of fabric to form a garment and/or by controlling and varying textile properties while weaving the fabric to be used in forming a garment.

The same ideas as for the fabrication of pants presented above, could also be applied to the fabrication of tops such as jackets, shirts, vests, gloves, hats, shoes or any other type

3

of garment suitable to be worn during the practice of extreme sports, or during the practice of a highly physically demanding activities.

Additional objects, advantages, and novel features of the invention will be set forth in part in the description which follows, and in part will become apparent to those skilled in the art upon examination of the following, or may be learned by practice of the invention.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING

The present invention is described in detail below with reference to the attached drawing figures, wherein:

FIG. 1 is an enlarged view of a twill weave, typical of denim fabrics.

FIG. 2 is an illustration of an exemplary loom where the warp yarns and the fill yarns used in the weaving of fabrics can be identified.

FIG. 3 is a perspective view of an exemplary denim fabric as it is being woven and rolled. Also, a schematic of a garment is shown on the fabric to show how a garment with multiple “performance zones” is constructed from a single fabric in accordance with the present invention.

FIG. 4 is an illustration of the constructed garment with the different “performance zones” in FIG. 3 shown as worn by an athlete.

FIG. 5A is a front view of the constructed garment with the different “performance zones” in FIG. 4 further comprising a gusset performance zone, shown as worn by an athlete.

FIG. 5B is a back view of the constructed garment with the different “performance zones” in FIG. 5A.

FIG. 5C is a perspective view of the constructed garment in FIG. 5A and FIG. 5B, showing the garment as worn by an athlete of BMX.

DETAILED DESCRIPTION OF THE INVENTION

Classic denim fabrics are made of 100% cotton fibers which provide advantageous properties such as good absorbency, comfortable soft hand and good color retention. However, 100% cotton denim fabrics are limited to the properties of cotton fibers which may not be stretchable, tend to retain water (making such fabrics slow to dry), shrink easily, retain soil, and tend to wear out faster than synthetic fibers. Therefore, an object of the present invention is to provide a cotton and synthetic fiber blend denim fabric that takes advantage of all the good traits of cotton fibers and at the same time, takes care of the disadvantages of cotton fibers by blending synthetic fibers.

Twill is a type of textile weave with the characteristic diagonal pattern observed in denim fabrics. Classic denim is a two faced “twill” construction fabric, as is illustrated in the piece of fabric 100 presented in FIG. 1. In classic denim, the front is considered to be the warp-face consisting mainly of the warp yarn 110 (usually tinted indigo blue to give “blue jeans” their distinctive color), and the back-face comprised mostly of the fill yarn 120 (usually left white). In the present description “yarn” is to be understood to be an assembly of fibers spun or twisted together to form a long and continuous string or filament useful for weaving or knitting fabric materials. The words “environment” and “environmental” are to be understood as the particular surfaces where athletes of extreme sports perform their activities, for example a skatepark for skateboarders usually comprising a series of

4

ramps and half pipes made of wood, cement, or synthetic construction materials. For FMX and BMX riders, the “environment” may comprise mountainous terrain, etc. Other types of extreme sports, and even day to day wear, may involve different environments.

In FIG. 2, an exemplary loom 200 is depicted. In a weaving process, warp yarns 210 are fed to the loom 200 from a warp beam 240 and finally rolled as the finished woven fabric 280 onto a fabric beam 250. The warp yarns 210 are kept tightened throughout the weaving process. A loom 200 typically has at least two “harnesses” 270 holding different sets of warp yarns 210. When one of the harnesses is lifted, a set of warp yarns is lifted and a v-shaped “shed” 290 is created in between the two sets of warp yarns 210. The fill yarn(s) 220 is then completely passed through the shed 290 via a shuttle 230 and then, the lifted harness is lowered. A comb like “reed” 260 is used to push the fill yarn(s) 220 tightly into place. Finally, when a different set of warp yarns 210 is lifted with a different harness, the fill yarn(s) 220 becomes trapped and interlaced forming the woven fabric 280.

It should be noted that there are different kinds of looms that may operate differently, especially modern day industrial looms. Modern day industrial looms, are automated and may or may not have shuttles carrying the fill yarn(s). Examples of modern day industrial looms are Water Jet looms, Air Jet looms, Shuttle looms, Rapier looms and Projectile looms. Water Jet and Air Jet looms are typically very fast because they do not require a shuttle to carry the fill yarn(s) across the warp yarns. Typically, when using Water Jet and Air Jet looms, the selvage on the fabric produced (the edges on either side of the fabric) is fringed because the fill yarn(s) is trimmed after insertion. Shuttle, Rapier and Projectile looms may be slower than Water Jet and Air Jet looms due to their higher requirement for mechanical action. However, fabrics produced with Shuttle, Rapier and Projectile looms have a finished selvage because they are produced from a continuous strand of fill yarn(s).

A first example denim fabric, hereinafter “moisture wicking denim” may possess moisture management capabilities by incorporating moisture wicking polymer fibers such as but not limited to Sorbtek® (available from Unifi). For example, Sorbtek® polyester fibers or any other polymer fibers with like properties may be incorporated in core spun yarns to be used as fill yarns. With the addition of moisture management polymer fibers in the moisture wicking denim in accordance with the present invention, when an athlete perspires, the moisture wicking denim fabric is able to pull the moisture produced on the surface of the athlete’s skin away from the athlete’s skin and subsequently facilitate evaporation of the moisture. By pulling away moisture from the athlete’s skin without retaining the moisture, the athlete may experience a continuous dry feeling, increasing the levels of comfort for the athlete.

When constructing the moisture wicking denim in accordance with the present invention, the warp yarns may comprise up to 100 weight percent cotton and carry the color for the final constructed denim fabric. The fill and/or warp yarns for the construction of the moisture wicking denim fabric of the present invention may also comprise additional synthetic fibers in the form of spandex or elastane, or any other elastic fiber usable in the construction of fabrics to add elasticity to the final moisture wicking denim fabric.

The moisture wicking denim fabric of the present invention may comprise up to 63 weight percent cotton fiber. For example, the moisture wicking denim fabric may comprise 40 to 63, 45 to 60, or 50 to 55 weight percent cotton fiber.

5

Further, the moisture wicking denim fabric of the present invention may comprise at least 35 weight percent moisture management polymer fibers and at least 2 weight percent elastic fibers.

A second example denim fabric, hereinafter “architecturally reinforced denim” may use high tenacity yarns integrated into the denim fabric for durability and strength. The high tenacity yarns of the present invention may incorporate synthetic liquid crystal polymer materials such as Vectran®, Kevlar®, Nomex®, Dyneema®, Twaron®, or the like, or any combination of different synthetic liquid crystal polymer materials suitable for the construction of fabrics. These synthetic liquid crystal polymer materials are desirable because they exhibit extraordinary physicochemical properties due to their unique crystalline like ordered state when melted or dissolved in a solvent. Processing these liquid crystal polymers into fibers or extrusion molded materials, gives rise to polymeric fibers or materials that have high resistance to chemical damage, wear and tear, puncturing, rupturing, and have great mechanical strength. The outstanding resilience properties of these synthetic polymer materials are a result of their self reinforcing properties at the molecular level deriving from the specific molecular organization and orientation of the molecules known as Van der Waals interactions. Another advantage of these types of synthetic polymer materials is their light weight and soft feel.

The fibers of the high tenacity polymer material for the manufacture of the architecturally reinforced denim of the present invention may be spun and incorporated directly into the cotton warp and/or the fill yarns. The fill yarns may also incorporate moisture management polymer fibers to add moisture management capabilities, as in the moisture wicking denim example presented earlier. Further, the high tenacity polymer material may be incorporated in the warp yarns, as the warp yarns go to the front face (exposed surface), which is the face directly subjected to the most environmental stress. Alternatively, the fibers of the high tenacity polymer materials may be spun into a 100 weight percent high tenacity polymer yarn. The 100 weight percent high tenacity polymer yarns may then be intercalated with up to 100 weight percent cotton yarns either as the warp and/or the fill yarns.

The architecturally reinforced denim example of the present invention may comprise up to 63 weight percent cotton fiber. The architecturally reinforced denim fabric may comprise 40 to 63, 45 to 60, or 50 to 55 weight percent cotton fiber. The architecturally reinforced denim fabric example of the present invention may comprise at least 35 weight percent synthetic and high tenacity synthetic polymer fibers and at least 2 weight percent elastic fibers, to increase elasticity and comfort, and improve fit when fabric is made into a garment.

The architecturally reinforced denim example of the present invention, in addition to its sturdiness, may also have an added visual and textural effect by having “wire” like motifs that correspond to the high tenacity yarns in the garment. The high tenacity yarns may optionally protrude from the front face of the denim weave, have different color, or otherwise be visually distinct from the other portions of a garment. However, such visual aspects of the high tenacity yarns are not necessary in garments in accordance with the present invention. For example, the motifs may be incorporated in the architecturally reinforced denim example by using the high tenacity synthetic polymer fibers in the warp and/or fill yarns taking advantage of the different look and feel that these fibers may have when compared to cotton fibers. Further, the motifs may be presented diagonally in the

6

same direction of the twill weave, the motifs may be continuously sequential, or the motifs may be spaced apart (spacing may be chosen according to the final desired visual and textural effect). In another example, the motifs may be woven into different shapes such as zig zag lines, curly lines, squares, circles, etc. Further, the motifs may be woven into particular designs or logos.

A third example denim fabric in accordance with the present invention, hereinafter “architecturally reinforced wicking denim” is further provided wherein properties of the moisture wicking denim through the moisture management fibers and the high tenacity polymer fibers are combined to provide a smooth, light weight, comfortable, dry feeling, resilient denim. The architecturally reinforced wicking denim example of the present invention provides outstanding resilience and protection against rips, and significantly slows down wear and tear even when exposed against repeated friction against harsh surfaces such as cement, rocks, sand, etc.

The architecturally reinforced wicking denim example of the present invention may comprise up to 63 weight percent cotton fiber. For example, the architecturally reinforced wicking denim example may comprise 40 to 63, 45 to 60, or 50 to 55 weight percent cotton fiber. The architecturally reinforced wicking denim fabric example of the present invention may comprise at least 35 weight percent of a combination of synthetic and high tenacity polymer synthetic fibers and moisture management fibers, and at least 2 weight percent elastic fibers, to increase comfort and improve fit when fabric is made into a garment.

The architecturally reinforced wicking denim of the present invention may further comprise other polymeric treatments such as “waterless wash,” or other finishing technologies suitable for the particular end use of the garment made from the denim of the present invention.

As briefly presented earlier, denim in accordance with the present invention may be used to manufacture different types of garments including tops (e.g. vests, jackets, shirts, blouses, etc), bottoms (e.g. pants, skirts, shorts, skorts, etc), gloves, pads, shoes, hats, etc. The garments may be made completely of one denim type in accordance with the present invention, or a combination of multiple denim types in accordance with the present invention. The garments may also be made from a combination of classic 100 weight percent cotton denim with one, or more types of denim in accordance with the present invention. The denim of the present invention when used in combination with other types of denim may be placed in strategic areas of the garments to maximize the specific characteristics of each type of denim.

For example, in the manufacture of pants for athletes of skateboarding, sandboarding, and/or competitive extreme rollerblading, the pants may be constructed completely of architecturally reinforced wicking denim to provide all best characteristics of moisture management and strength. Additionally, the pants may discretely comprise padding in the areas of the buttocks and the knees to provide shock absorption in case of a fall.

In another example of athletic denim pants, the area of the waist line may be comprised of the moisture wicking denim example where the pants come in closest contact with the body. The areas of the buttocks and the knees may comprise the architecturally reinforced denim example to provide visual appeal and added strength and resilience to these areas, which are subjected to greater stress both from the movement of the athlete and from contact with environmental stressors. The rest of the pants may comprise classic stretchable, and/or classic non-stretchable lightweight

7

denim, and/or architecturally reinforced wicking denim, and/or any other type of denim or even other fabrics. These different denim types in different performance zones of the garment may, for example, be welded and/or stitched together to construct the final garment.

In a different example, multiple types of denim may be woven at different locations on a textile that will be formed into a garment to create different performance zones. For example, the moisture wicking denim and the architecturally reinforced denim examples may be woven into different performance zones of the same fabric piece. Yet, in another example, the moisture wicking denim and the architecturally reinforced wicking denim examples may be woven into different performance zones of a single fabric piece. Further, the architecturally reinforced wicking denim and the architecturally reinforced denim examples may be woven into different performance zones of a single fabric piece, or yet in another example, all three denim types, i.e. the moisture wicking denim, the architecturally reinforced denim and the architecturally reinforced wicking denim may be woven into different performance zones of a single fabric piece.

In yet a further example, a full body garment for a BMX or FMX athlete may be constructed from one or a few pieces of fabric woven into different performance zones. First, the areas corresponding to the elbows, chest, crotch, buttocks and knees of an athlete may be woven into the architecturally reinforced denim in accordance with the present invention to provide extra resilience in those areas. Second, the areas corresponding to the back and thighs may be woven into the architecturally reinforced wicking denim of the present invention to provide comfort and resilience by wicking away perspiration from these areas. Finally, the areas of the armpits and the rest of the garment may be woven into the moisture management denim, where resilience is not as crucial as moisture management.

Shown in FIG. 3 is a section of a loom 300 weaving a denim fabric 320 with different performance zones in accordance with the present invention. The warp yarns 310 are fed from warp beam 340 and the fill yarn(s) is fed according to the loom type (not shown). The fabric piece 320 shown in FIG. 3 has a first performance zone 321, a second performance zone 323, a third performance zone 325, a fourth performance zone 327, and finally a fifth performance zone 329 woven into it.

In the example shown in FIG. 3, a zoned denim fabric for the construction of pants 350 for an athlete of extreme sports is shown. The example illustrated by FIG. 3 is not necessarily to scale. For example, multiple garment pieces may be cut from a single width of fabric woven in accordance with the present invention. The different types of fibers needed for the different performance zones of the final fabric piece may be introduced through the warp yarns and/or the fill yarns. If the different types of fibers are introduced through warp yarns, warp yarns having different types of fibers along their length may be used. The presence of each different type of fiber along the warp yarns' lengths may be predetermined according to the specifications of the final fabric product. If the different types of fibers are introduced through the fill yarn(s), the fill yarn(s) may be spliced with the yarn containing the next type of polymer fiber desired.

In FIG. 3, only one cut is made for the construction of a garment. However, depending on the width of the zoned denim fabric, several garments could be cut out along the width of the zoned denim fabric in accordance with the present invention. The position of performance zones along the length and/or width of a textile should be accorded for in laying out and/or cutting pieces for forming garments in

8

accordance with the present invention. For example markers denoting transitions between performance zones may be temporarily or permanently applied to the textile, woven into the textile, etc. Alternatively/additionally, different types of performance zones may be distinguishable from one another. Markers and/or performance zones themselves may be perceived by an unaided human, an aided human (for example using black light), or may be detected by automated sensors. By way of further example, computer software operating on a computing device may coordinate weaving and cutting operations to assure the proper location of performance zones in the final garment.

Continuing on the discussion of FIG. 3, a denim fabric for the fabrication of athletic pants 350 with different performance zones woven in to it is provided. Performance zone 321 may also be thought of as a waist performance zone and may be woven into a moisture wicking denim fabric by supplying the moisture management fibers through the fill yarn(s) and/or the warp yarns to provide moisture management comfort along the waistline of pants 350. Performance zone 323 may also be thought of as a buttocks performance zone and may be woven into an architecturally reinforced denim fabric to provide protection and durability in the area of the buttocks. The high tenacity fibers may be supplied mainly through the warp yarns to place the high tenacity fibers on the external face of the garment. Performance zone 325 may also be thought of as a thigh performance zone and may be woven into an architecturally reinforced wicking denim fabric with both the moisture management fibers and the high tenacity fibers incorporated. Performance zone 327 may also be thought of as a knee performance zone and may again be woven into an architecturally reinforced denim fabric like in the buttocks performance zone 323 to provide the protection and durability in the knee area. Performance zones 323 and 327, which are subjected to high levels of stress both from the environment and the physical exertion of the athlete may need extra reinforcement and thus, may comprise up to 100 weight percent high tenacity synthetic polymer fibers. Finally, performance zone 329 may also be thought of as a calf performance zone and may be woven into a classic denim fabric since performance zone 329 is subject to the least amount of stress when pants 350 are worn by the athlete. In yet a further example, a full body garment for a BMX or FMX athlete.

FIG. 4 is an exemplary illustration of constructed pants 350 from the zoned denim fabric presented in FIG. 3, as worn by an athlete. As can be observed in FIG. 4, the waist performance zone 321 corresponds to the waistline of the athlete, the buttocks performance zone 323 corresponds to the buttocks area of the athlete, the thigh performance zone 325 corresponds to the thighs of the athlete, the knee performance zone 327 corresponds to the knees of the athlete, and finally, the calf performance zone 329 corresponds to the calves of the athlete and extends downward towards the ankles of the athlete.

FIG. 5A through FIG. 5C show a further example of constructed pants 350 from the zoned denim fabric presented in FIG. 3, as worn by an athlete such as a BMX athlete. Pants 350 in FIG. 5A through FIG. 5C are constructed with the same performance zones as the pants 350 presented in FIG. 4 except, in FIG. 5A through FIG. 5C, the pants 350 further comprise an extra tough and resilient gusset performance zone 322 corresponding to the crotch area when pants are worn. The gusset performance zone 322 in pants 350 may be subject to constant friction from the contact with the seat of a bike, and thus the need for extra

9

protection in this area may be necessary for better protection of the athlete and durability of pants **350**.

FIG. 5A is a front view of pants **350** as worn by an athlete. As can be observed in FIG. 5A, the waist performance zone **321** corresponds to the waistline of the athlete, the buttocks performance zone **323** corresponds to the hip area of the athlete on the front, the thigh performance zone **325** corresponds to the thighs of the athlete, the gusset performance zone **322** corresponds to the crotch area of the athlete, the knee performance zone **327** corresponds to the knees of the athlete, and finally, the calf performance zone **329** corresponds to the calves of the athlete and extends downward towards the ankles of the athlete. Further, the gusset performance zone may extend partially (as shown) or completely around the leg of the athlete (not shown).

FIG. 5B is a back view of pants **350** as worn by an athlete. As can be observed in FIG. 5A, the waist performance zone **321** corresponds to the waistline of the athlete, the buttocks performance zone **323** corresponds to the buttocks area of the athlete on the back, the thigh performance zone **325** corresponds to the thighs of the athlete, the gusset performance zone **322** corresponds to the crotch area of the athlete, the knee performance zone **327** corresponds to the knees of the athlete, and finally, the calf performance zone **329** corresponds to the calves of the athlete and extends downward towards the ankles of the athlete. Further, the gusset performance zone may extend partially (as shown) or completely around the leg of the athlete (not shown).

FIG. 5C is a perspective view of a BMX athlete sitting on a bike and wearing pants **350**. FIG. 5C shows with more clarity how the different performance zones may play an important role in protecting the athlete and, at the same time, insuring the comfort of the athlete when the pants **350** are worn.

Since the different performance zones in a zoned denim fabric in accordance with the present invention are very specific and must be localized properly in the final garment, extra care may be taken when cutting out the fabric and then constructing the desired garment. Alternatively, the denim fabric may have a fixed width corresponding exactly to the length of the garment. Then, the different performance zones may be woven vertically along the fabric's length such that the cuts for the garments may be taken horizontally. In other words, the zoning set up shown in FIG. 3 may be rotated 90 degrees such that the different zones appear from left to right, or right to left, as opposed to from top to bottom (as shown). In addition to being visually appealing, apparel made from a single fabric with different performance zones may be more comfortable since the need for bulky stitching between two or more fabrics when trying to create a garment with different properties in different areas would be eliminated. Reducing the amount of stitching needed to create a garment with different properties in different areas also makes a more durable garment since the chances of the garment coming apart if the stitches become undone may be reduced.

Single fabric pieces comprising two or more denim types woven together, may be custom woven to manufacture custom made garments or protective gear that fit the specific needs of the user, and specific to the particular sport or activity to be engaged in. Also, whether the zoning setup is done along the fabrics length or across the fabric's length, different permutations of the zones may be possible. The specific zone lengths and frequencies may be adjusted according to the needs for the specific garments to be constructed.

10

Further, the garments or protective gear comprising the denim of the present invention may be woven using dual-loom technology to create seamless garments and protective gear. For example, in the manufacture of gloves, the palm-side may be woven into an architecturally reinforced wicking denim fabric and the back side may be woven into an architecturally reinforced denim fabric. This combination would result in a strong, flexible and moisture absorbent glove on the palm-side (where sweat gathers) and a strong, flexible and protective glove on the back side. This dual-loom weaving could also be applied to other garments such as pants, shorts, vests, shoes, socks, etc., choosing the right type of denim for different areas of choice. This may be done with any combinations and permutations of architecturally reinforced wicking denim, architecturally reinforced denim, moisture wicking denim, classic stretchy, and/or classic non-stretchy denim. Further, the names, compositions and/or properties of these three examples of denim in accordance with the present invention are for illustrative purposes only.

As one may also be able to conceive, the possibilities presented above may be applied to other types of fabrics as well, not being limited to denim.

From the foregoing, it will be seen that this invention is one well adapted to attain all the ends and objects hereinabove set forth together with other advantages which are obvious and which are inherent to the structure.

It will be understood that certain features and subcombinations are of utility and may be employed without reference to other features and subcombinations. This is contemplated by and is within the scope of the claims.

Having thus described the invention, what is claimed is:

1. An architecturally reinforced denim woven fabric comprising:

a first face and an opposite second face, wherein the first face is different from the opposite second face;

at least a first woven performance zone comprising a first ratio of synthetic fiber to natural fiber, wherein the first woven performance zone is positioned at a first location on the architecturally reinforced denim woven fabric, wherein the first woven performance zone comprises:

- (1) up to a 63 weight percent cotton fiber;
- (2) at least a 35 weight percent combination of moisture management polymer fiber and high tenacity polymer fiber, wherein the high tenacity polymer fiber is in one or more warp yarns, and wherein the moisture management polymer fiber is in one or more fill yarns of the architecturally reinforced denim woven fabric and wherein the one or more warp yarns are exposed on the second face and the one or more fill yarns are exposed on the first face; and

- (3) at least a 2 weight percent elastic polymer fiber; and at least a second woven performance zone comprising a second ratio of synthetic fiber to natural fiber, wherein the first ratio of synthetic fiber to natural fiber is different than the second ratio of synthetic fiber to natural fiber, and wherein the second woven performance zone is positioned at a second location on the architecturally reinforced denim woven fabric such that it is integrally woven and seamlessly adjacent to the first woven performance zone.

2. The architecturally reinforced denim woven fabric of claim **1**, wherein the second woven performance zone comprises:

- up to a 63 weight percent of the cotton fiber;
- at least a 35 weight percent of the high tenacity polymer fiber; and
- at least a 2 weight percent of the elastic polymer fiber.

US 9,624,608 B2

11

3. The architecturally reinforced denim woven fabric of claim 2, wherein the architecturally reinforced denim woven fabric further comprises a third woven performance zone, the third woven performance zone comprising a 100 weight percent cotton fiber.

4. The architecturally reinforced denim woven fabric of claim 1, wherein the first face of the architecturally reinforced denim woven fabric is configured to be an internal face of a manufactured garment and the opposite second face of the architecturally reinforced denim woven fabric is configured to be an external face of the manufactured garment.

5. The architecturally reinforced denim woven fabric of claim 4, wherein the warp yarns are visually distinct from other portions of the architecturally reinforced denim woven fabric.

6. An architecturally reinforced denim woven fabric comprising:

at least a first woven performance zone comprising a first ratio of synthetic fiber to natural fiber, wherein the first woven performance zone is positioned at a first location on the architecturally reinforced denim woven fabric, wherein the first woven performance zone comprises:

- (1) up to a 63 weight percent cotton fiber;
- (2) at least a 35 weight percent high tenacity polymer fiber, wherein the high tenacity polymer fiber is incorporated into one or more warp yarns of the architecturally reinforced denim woven fabric; and
- (3) at least a 2 weight percent elastic polymer fiber; and

at least a different second woven performance zone comprising a second ratio of synthetic fiber to natural fiber, wherein the first ratio of synthetic fiber to natural fiber is different from the second ratio of synthetic fiber to natural fiber, and wherein the second woven performance zone is positioned at a second location on the architecturally reinforced denim woven fabric, wherein the first location is different from the second location, and wherein the first woven performance zone and the second woven performance zone are integrally woven and are seamlessly adjacent to each other.

7. The architecturally reinforced denim woven fabric of claim 6, wherein the first woven performance zone comprises between 45 and 60 weight percent cotton fiber.

8. The architecturally reinforced denim woven fabric of claim 6, wherein the high tenacity polymer fiber comprises liquid crystal polymer materials.

9. The architecturally reinforced denim woven fabric of claim 6, wherein the second woven performance zone comprises a 100 weight percent cotton fiber.

10. The architecturally reinforced denim woven fabric of claim 6, wherein the warp yarns comprising the high tenacity polymer fiber form one or more protrusions on an external surface of the architecturally reinforced denim

12

woven fabric that are visually distinct from other portions of the architecturally reinforced denim woven fabric.

11. A garment manufactured from an architecturally reinforced denim woven fabric, the garment comprising seamlessly adjacent and integrally woven performance zones, wherein:

a first woven performance zone comprising a first ratio of synthetic fibers to natural fibers, wherein the synthetic fibers comprise high tenacity polymer fibers forming one or more warp yarns;

a second woven performance zone comprising a second ratio of synthetic fibers to natural fibers that is different from the first ratio of synthetic fibers to natural fibers, wherein the synthetic fibers comprise moisture management polymer fibers and high tenacity polymer fibers, wherein the moisture management polymer fibers form one or more fill yarns and the high tenacity polymer fibers form one or more warp yarns; and

a third woven performance zone comprising a third ratio of synthetic fibers to natural fibers that is different from the first ratio and the second ratio of synthetic fibers to natural fibers.

12. The garment of claim 11, wherein the first woven performance zone of the garment is configured to form a thigh and knee performance zone configured to align with the thighs and knees of a wearer when the garment is worn; wherein the second woven performance zone of the garment is configured to form a buttocks performance zone configured to align with the buttocks of the wearer when the garment is worn; and wherein the third woven performance zone of the garment is configured to form a calf performance zone configured to align with the calves of the wearer when the garment is worn.

13. The garment of claim 12, wherein the buttocks performance zone and the knee performance zone further comprise padding for shock absorption.

14. The garment of claim 11, wherein the first woven performance zone and the second woven performance zone comprise up to a 63 weight percent of cotton fiber, and the third woven performance zone comprises 100 weight percent of the cotton fiber.

15. The garment of claim 11, wherein the garment comprises an internal face and an external face, wherein the high tenacity polymer fiber in the first performance zone and the second performance zone is mainly located on the external face of the garment.

16. The garment of claim 15, wherein a portion of the warp yarns comprising the high tenacity polymer fiber form one or more protrusions on the external face of the garment, wherein the one or more protrusions are visually distinct from other portions of the external face of the garment.

* * * * *

WWD


BUSINESS / TECHNOLOGY

Nike's New Patent Could Mark the Rise of Ath-Denim

The athletic multinational got its first denim patent this week.

By [Kali Hays](#) on April 21, 2017



 Nike, best known for athletic shoes and gear, has secured a patent for performance denim.
Lexie Moreland

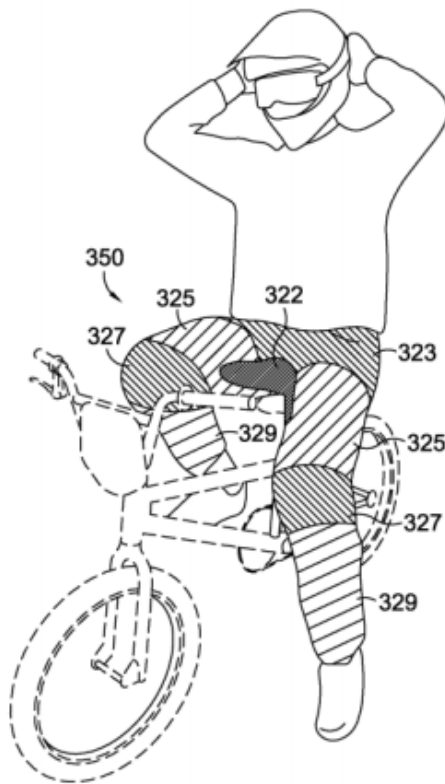
NEW YORK — Denim and athleticwear may seem an unlikely fit, but Nike could be the brand to change that.

Earlier this week, the activewear giant secured a utility patent for “architecturally reinforced denim” that essentially describes a jeans-jogging pant hybrid, meaning “ath-denim” could be coming to a Nike store near you.

During a recent call with analysts discussing its positive 2016 financial results, Nike president and chief executive officer Mark Parker said the company planned to continue its “relentless flow of innovation” in order to sustain momentum.

The new patent appears to be in line with that promise. It describes a denim fabric that offers “high tenacity” and “moisture management” along with stretch in differing proportions, depending on the desired performance.

Pants made from the fabric are said to have separate but seamless “performance zones,” with the buttocks, thigh and calf areas all likely to have differing fabric weaves, plus “padding for shock absorption.”



An image from Nike’s new patent details “performance areas” of athletic pants made with the denim.

Nike offers a small range of men’s pants, including one denim option geared toward skateboarders, but the new patent is aimed at extreme sports such as BMX and motocross.

“For decades now, denim has been a popular ‘American comfort’ staple in everyone’s closet, both in the U.S. and around the world,” Nike said in its patent application. “While denim is a

relatively tough and durable fabric, conventional denim lacks the resilience and other performance and/or comfort characteristics desired for athletic endeavors, particularly extreme sports.”

With the new patent, Nike said it hopes to offer “denim fabric and gear made from this fabric suitable for extreme sports athletes, providing them with comfort and an outstanding level of protection, while being fashionable and attractive.”

Nike said the denim fabric could be used in the manufacture of all other types of apparel, from women’s leggings to shoes, and noted the fabric can be dyed any color, not just blue.

Moreover, Nike said the combination of synthetic polymers in the fabric would not only create a “lightweight, comfortable, dry feeling, resilient denim” but also one that provides “outstanding resilience and protection against rips, and significantly slows down wear and tear even when exposed against repeated friction against harsh surfaces such as cement, rocks, sand, etc.”

Future iterations of the fabric could offer a “waterless wash,” according to the application, which also alluded to the possibility of fabrics beyond denim getting the same composition.

While Nike is a prolific patent filer, this appears to be the company’s first for denim. Nike initially filed for the patent in 2012.

The company could not be immediately reached for comment.

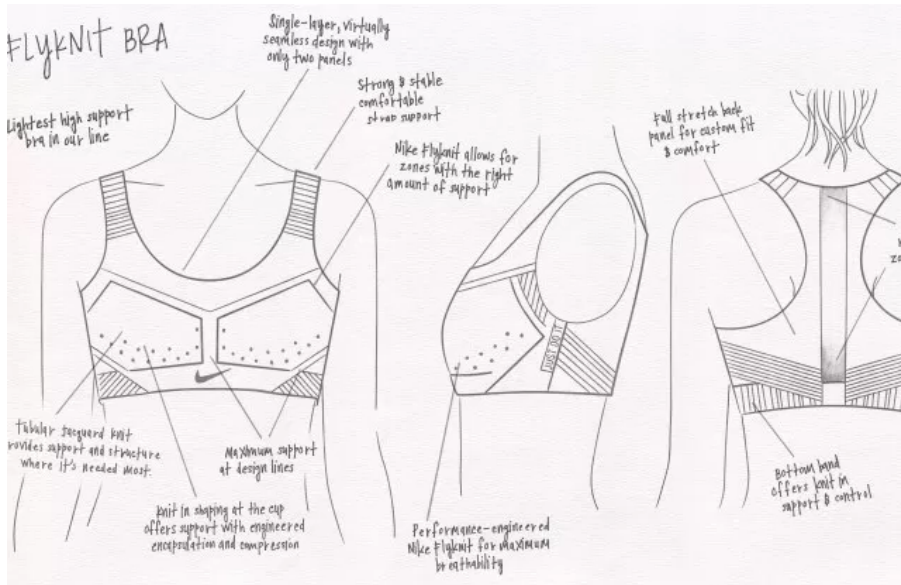


FASHION / ACTIVEWEAR

Nike Just Does It: Applies Footwear Technology to Apparel

Activewear giant finds new uses for older manufacturing process.

By [Sharon Edelson](#) on July 12, 2017



📷 An illustration of the benefits of Nike's Flyknit bra.

Nike today is launching the Fe/Nom bra, the first apparel product to use Flyknit technology, which until now has been reserved for footwear.

“We’re going to apply the benefits across Nike apparel,” said Nicole Rendone, senior bra innovation designer at Nike. “We’ll continue to expand bras and all apparel, including leggings and socks. Flyknit could be used in anything. We think it’s huge. This is only the beginning.”

The new bra offers flexibility, breathability and conforms to the body in the same way that Flyknit conforms exactly to the shape of a foot.

“This changes everything for us and for women,” said Rendone. Asked why Nike chose a bra for its first Flyknit apparel product, Rendone said, “It’s an essential item. We felt the bra had the ultimate benefit and the largest challenge. We also thought the bra was the most exciting place to start.”

Nike Flyknit, which bowed at the 2012 London Summer Olympics with the Nike Flyknit Racer, is a digitally-engineered knitting process used in lightweight, formfitting and virtually seamless shoe uppers. The technology is used in Nike sport footwear including the Zoom Fearless Flyknit women’s training shoe and Kevin Durant’s signature Nike KD10.

For the new bra, engineers and designers logged more than 600 hours of biometric testing on women in a variety of shapes and sizes and created atlas maps, which involve digital body scans to find areas of high heat, sweat, cooling and movement.

The Nike team was able to significantly reduce the materials and seams in the Fe/Nom bra. “We looked at high support bras and all the elements,” Rendone said. “Other high-support Nike bras can have up to 41 pieces and 22 seams. The Fe/Nom Flyknit bra has two panels and a binding and is 30 percent lighter than any other bra in Nike’s line.”

Flyknit enabled Nike to put components such as encapsulation and compression in a single knit panel. Using different knit structures and densities, designers were able to supply control and support without the use of components such as wires, pads, stabilizers and elastics.

“If you think of the components, they’re the major points of irritation,” Rendone said. “Bonded-on components and elastic bands are common sources of irritation. Our bands are really thin.”

Constructed with an ultra-soft nylon-spandex yarn that conforms to the body, the Fe/Nom uses two single-layer panels that are assembled for a seamless feel.

Rendone pointed out that Flyknit is environmentally friendly.

“Knitting is very sustainable and produces minimal waste,” she said. “When you knit, it’s not like you’re cutting away fabric and throwing pieces away.”

The \$80 Nike Fe/Nom Flyknit bra is being sold exclusively for 48 hours on the Nike+ app. After that it will be available on nike.com. The bra in October will launch worldwide and eventually roll out to stores.

Rendone explained that the bra, which comes in sizes XS to XL, is available in only one colorway for now. “We didn’t want to wait for other colors to put this on the market,” she said. “Future styles and colors will be coming and are in the works already.”

The designer is her own testimonial. “I ran six miles in the bra and I’ve worn it as a top,” she said. “You feel like you’re wearing nothing. It’s a bra you’ll want to wear all day long.”



VIBRATING CONNECTED JEANS

THEY ARE ESSENTIAL, JUST LIKE THE IMPORTANT INFORMATION THAT YOU DO NOT WANT TO MISS.

Equipped with two vibrating sensors on the belt and connected to your smartphone via Bluetooth, this product offers new features that integrate into your daily life.

The geolocation feature allows you to navigate through your urban settings using guiding vibrations either on the right or left side of your Vibrating Connected Jeans.

This technology provides an easier, and above all more intuitive option to help you find your car or your meeting place, for example.

More fun features called "Ping" will satisfy those who want to interact with their surroundings through vibration that can be customized in terms of duration, frequency and intensity. This is useful for when you want to discreetly attract someone's attention, or for open offices, or for students. The system can also be programmed to inform you if you are running late. With its integrated push button, this clothing of the future has numerous uses: security alerts, home support, geolocation of your children, a solution for the problem of isolated workers, etc.



FIGHTING AGAINST BURNOUT

Active managers and others looking for a solution to combat burnout of constantly looking at a phone screen will find the system particularly interesting. Indeed, the associated application allows you to

configure your email settings so that the sensors will only vibrate in the case of very important **129** information.

This function eliminates the need to constantly check your phone, thus putting a technological buffer between your connected life (email, SMS, phone, chat, etc.) and your need to concentrate and relax while still remaining available for essential matters (for emergency messages from children, or for receiving necessary information, for example).

AND THE MATERIAL COMES ALIVE :

The integration of electronics into the same fabric offers a new experience of clothing use. The fabric comes alive and takes care of interacting with the connected world to bring you new and unique sensations.

Vibrating Connected Jeans : a new method for linking the digital with design that interests both women and men who are into new technologies, but also appeals to those who are not yet aware of this new, creative, high-end project.





THE CONNECTED VIBRATING JEANS UNDERSTAND YOUR BEHAVIOR :

With the aim of optimizing the battery life, the Connected Vibrating Jeans have been programmed to stay in sleep mode when they aren't used. As soon as we wear them, they wake up and they connect with your Smartphone.

If you don't wear them, they fall asleep again and set in sleep mode.

The Connected Vibrating Jeans were even programmed especially to be able to detect if it is in a washing machine to stay in sleep mode even if it is in movement within the framework of the wash.

So the Connected Vibrating Jeans can be used, with all connected functions, during four years (if worn once per week) without having to change or charge the battery.

MADE-IN-FRANCE PRODUCTS IN THE SPOTLIGHT :

SPINALI DESIGN remains true to its high-end background and is relaunching the denim sector in France! Design, application development (for Android and iOS smartphones), and medical research is all done in Mulhouse, France.

The jeans were developed in Alsace. The fabrics, the clothing, and the electronics are all made in France. Several denim models, such as a skirt, two types of jeans, two types of shorts, and two jackets, have been carefully designed to meet the needs of all active people. The range also has something for men, with jeans specially designed for those with an active lifestyle.



“BE NICE, BE REBEL, BE YOURSELF.”

True to its slogan, and in an attempt to banish clichéd ideas of the perfect woman, the brand SPINALI DESIGN continues to use only non-retouched photos to promote its Vibrating Connected Jeans: a new policy to help women banish their imperfections and feel at home with the brand

LIVE THE EXPERIENCE OF THE VIBRATING CONNECTED JEANS

A B O U T

Before being CEO of SPINALI DESIGN, Marie SPINALI obtained her law degree. After the birth of her three daughters, she resumed her studies to obtain a web designer degree. She worked hard and became a manager of a computer company in an already very technological universe. A strong desire to work in the intelligent design sector resulted in the creation of SPINALI DESIGN in 2015.

Everything started from a vision :

While the founder of SD, Marie Spinali, was on vacation near the Italian town of Neviano, she saw someone getting a sunburn. She began to wonder, what could be better than a swimsuit that tells you when to reapply sunscreen?

It is the woman who can affirm her femininity while putting forward her skills and her intelligence. The image that SPINALI DESIGN puts forward is very important as it reflects the place of woman in society; it is even more important for Marie SPINALI because she has three daughters. She wants to show them that a woman can be can "Be Nice. Be Rebel. Be Yourself."

True to its slogan, and in an attempt to banish clichéd ideas of the perfect woman, the brand SPINALI DESIGN continues to use only non retouched photos to promote its ESSENTIAL Jeans: a new policy to help women banish their imperfections and feel at home with the brand!

The SD adventure began with our NEVIANO, connected bathing suits using highly technical UV sensors that are connected to the Smartphone to help avoid sunburn.

As we progressed, we affirmed our ambition to be the leader of the connected smart clothing by developing a range of dresses equipped with sensors that allow a woman to interact with her entourage.

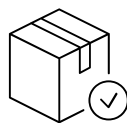
On September 19, 2016, we launched the Essential Women's Vibrating Jeans in New York. Equipped with 2 vibrating sensors at the level of the belt and connected to a Smartphone, they will offer new functions like the guidance in the urban routes or to avoid the burn out of constantly looking at a phone screen. We therefore have the chance to revitalize the jean sector in France.

Marie combines her two passions, technology and design, by creating the first connected swimsuits of Europe. She hopes to show women that they can be a CEO of a company. She loves

being an example to her team full of young women. Marie Spinali has overcome obstacles and stereotypes of women in the workforce. She hopes to continue to break down barriers women face with her brand Spinali Design. **133**

SPINALI DESIGN

"Be Nice, Be Rebel, Be Yourself"



**WORLDWIDE
DELIVERY**

F.I.T.: FASHION AS INFORMATION TECHNOLOGY

Susan Scaffidi[†]

CONTENTS

INTRODUCTION	69
I. PATTERNS OF INFORMATION.....	71
II. WEAVING TALES AND SPINNING YARNS: A HISTORICAL PERSPECTIVE.....	75
III. LAYERED LOOK: THE DUAL NATURE OF FASHION AS A COMMUNICATIONS MEDIUM.....	79
IV. A CUTTING-EDGE LEGAL APPROACH TO FASHION AS INFORMATION TECHNOLOGY.....	82
A. <i>So Last Season: The Legal Status Quo</i>	82
B. <i>Trend Report: Tailoring Law to Fit Creators and Consumers</i>	87

INTRODUCTION

Before you begin reading, pause for a moment to picture an example of information and communications technology. Perhaps the first thing that came to mind was your laptop, iPod, or new mobile phone. Whatever image you envisioned, it probably wasn't a 100,000-year-old necklace,¹ a nineteenth-century loom,² or the latest designer handbag—yet those clothing and textile-related items exhibit the same information-related capacities as their digital descendants.

The use of technology to manage, process, or communicate information is a defining characteristic of the modern era. Even as digital technologies have become more prevalent in our lives, however, the

[†] Visiting Professor, Fordham Law School; Associate Professor of Law and Adjunct Professor of History, Southern Methodist University. The author would like to thank Professors Lisa Dolak and Keith Bybee and the staff of the *Syracuse Law Review* for the invitation to participate in the “Creators v. Consumers” symposium, as well as Laurence Abraham and Ariana Lindermayer for research assistance. Additional discussion of issues relating to law and fashion is available on the author’s website, <http://www.CounterfeitChic.com>.

1. See Marian Vanhaeren et al., *Middle Paleolithic Shell Beads in Israel and Algeria*, 312 *SCI. MAG.* 1785-88 (2006) (discussing the discovery of ancient jewelry and its significance).

2. See generally JAMES ESSINGER, *JACQUARD’S WEB: HOW A HAND-LOOM LED TO THE BIRTH OF THE INFORMATION AGE* (2004).

popular conception of “information technology”—and thus its scope as a tool of cultural and legal analysis—has narrowed.³ We suffer from a sort of digital blindness, able to draw upon and interpret the multiplicity of information sources surrounding us, but reluctant to analyze them according to the prevailing information technology paradigm.

At the same time that we have limited our focus with respect to information technology, we have elevated its importance in formulating the legal policies that promote creativity and regulate access to the means of production in the new Information Age.⁴ The spread of Internet communications has prompted increases in intellectual property protection for those with established creative investments,⁵ as well as arguments that such legal interference is a threat to evolving forms of expression.⁶ Debates over access to technology, including network neutrality, have developed along similar lines. Indeed, no reasonable person could deny that the rapid spread of new technologies over the past few decades requires careful attention and thoughtful analysis. The conceptual restriction of information technology to recently created digital platforms, however, unnecessarily confines our understanding of the broader phenomena of communication and dissemination of information and thus our ability to manage them productively.

The goals of this essay are twofold: first, to redirect attention to the broader realm of information and communications technology, of which fashion is a foundational medium; and second, to analyze fashion as an information technology in order to better understand the industry’s desire for intellectual property protection, popular resistance to such protection, and the most efficacious balance between them in terms of creative expression. My long-term research has focused on cultural and historical reasons for the limited degree of intellectual property protection extended

3. Over a decade ago, James Boyle offered a caution against unnecessarily narrow definitions of information itself, noting that it “does not need to be stored in ones and zeroes.” JAMES BOYLE, SHAMANS, SOFTWARE, AND SPLEENS: LAW AND THE CONSTRUCTION OF THE INFORMATION SOCIETY 4 (1996).

4. See generally Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX L. REV. 553 (1998) (offering early insight into the necessary integration of technology and policy).

5. E.g., Digital Millennium Copyright Act of 1998, Pub. L. No. 105-304, 112 Stat. 2860 (codified as amended in scattered sections of 17 U.S.C.).

6. Many significant works have raised structural concerns about the relationship between law and information production. See generally, e.g., YOCHAI BENKLER, *THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM* (2006); LAWRENCE LESSIG, *FREE CULTURE: HOW BIG MEDIA USES TECHNOLOGY AND THE LAW TO LOCK DOWN CULTURE AND CONTROL CREATIVITY* (2004); JESSICA LITMAN, *DIGITAL COPYRIGHT* (2001).

in the past to certain categories of human creativity, including fashion design.⁷ This essay turns to the question of why—despite shifting cultural attitudes and other conditions—some tension still exists between creators and consumers of fashion, how information theory can contribute to an explanation for that tension, and what role law can play in its resolution.

Beginning with Part I, the following pages explore the definition of information and communications technology and its legal parameters. Turning specifically to the clothing and textile industry, Part II focuses on both the historical role of fashion in conveying information and the production mechanisms that are direct historical antecedents of more recently developed information technologies. Part III discusses the bi-level nature of clothing and accessories as information technology; simultaneously embodying the designer's authorial voice and generating information on behalf of and about the wearer. Finally, Part IV identifies the dueling approaches to intellectual property law inherent in fashion's dual information identity and suggests a framework for their resolution.

Fashion, in simplest terms, is not merely an information technology, but an ancient, universal, and complex information technology. By examining it according to this rubric, we can gather insight into not only the concept of such technologies but also the particular characteristics of fashion that influence its relationship to intellectual property law. That fashion is a creative and communicative medium is a longstanding characteristic of human culture; that U.S. law must finally recognize it as such is a rational unfolding of information policy.

I. PATTERNS OF INFORMATION

Outside of the legal context, scholars invoke an expansive view of information technology to describe and understand a range of phenomena far beyond the telecom industry.⁸ Nothing is too vast or too minute, too simple or too complex, to function in an information theory context. Within the realm of human interaction, information exchange is the medium that can bind a culture together or, in its absence, result in chaos and collapse. Understood from this perspective, information processing is a vital function, and the law plays an important role by managing the flow of information and protecting the strength and clarity of individual

7. See generally SUSAN SCAFIDI, WHO OWNS CULTURE?: APPROPRIATION AND AUTHENTICITY IN AMERICAN LAW (2005); SUSAN SCAFIDI, COUNTERFEIT CHIC: THE REAL STORY OF FAKE FASHION (forthcoming 2009).

8. See, e.g., SETH LLOYD, PROGRAMMING THE UNIVERSE: A QUANTUM COMPUTER SCIENTIST TAKES ON THE COSMOS 3 (2006).

messages. Massachusetts Institute of Technology computer scientist Seth Lloyd, in his recent work *Programming the Universe*, observes that the universe itself is a natural form of information technology—“[e]very . . . particle registers bits of information [and e]very interaction between those pieces of the universe processes that information by altering those bits.”⁹ The patterns generated through this process give rise to new computational forms, from stars and planetary ecosystems to human language and culture, “a true information-processing revolution that has substantially changed the face of the Earth.”¹⁰

Lloyd’s research points to an important distinction between scientific and popular notions of information technology. As Charles Seife notes in his recent overview of information research, “The word *information* conjures visions of computers and hard drives and Internet superhighways; after all, the introduction and popularization of computers came to be known as the information revolution. However, computer science is only a very small aspect of an overarching idea known as information theory.”¹¹

To understand why, it is necessary to look past the narrow boundaries of information technology as the term is used by technicians and telecommunications experts. At the most fundamental level, information is a property of physical existence.¹² In Lloyd’s words, it is the means by which “one physical system . . . can be put into correspondence with another physical system.”¹³ Just as a computer language enables a laptop to convert keystrokes into paragraphs, the information in a particle shapes the distinct properties that we observe and measure.¹⁴ In the natural world, information processing determines the contours of all physical objects, from the heat of the sun to the ice in the tundra, as well as the changes that emerge when these objects interact.¹⁵

Our perception of the power of information processing has given rise to a diverse array of communications technologies designed to relate and transform. Perhaps the most familiar is abstract symbolic language, a communications medium that most people use every day.¹⁶ As with telephony, the medium in which Claude Shannon first elaborated the core

9. *Id.*

10. *Id.* at 209.

11. CHARLES SEIFE, *DECODING THE UNIVERSE: HOW THE NEW SCIENCE OF INFORMATION IS EXPLAINING EVERYTHING IN THE COSMOS, FROM OUR BRAINS TO BLACK HOLES 1* (2006) (emphasis in original).

12. *See* LLOYD, *supra* note 8, at 65.

13. *Id.* at 27.

14. *See id.* at 27-37.

15. *Id.* at 38-61.

16. *Id.* at 13.

principles of modern information theory,¹⁷ language raises the question of how to transmit information efficiently without the message degrading into incoherence.¹⁸ In this regard, grammar serves as an information technology that encodes optimal arrays for organizing semantic values. At a more basic level, the human voice is an information processing “technology” that itself “makes language possible” and in doing so facilitates “the uniquely human forms of social organization that have made our species so successful thus far.”¹⁹

Human language may be a ubiquitous mode of encoding information, but it is by far not the only one. Before information technology became synonymous with electronic computing in the popular mind, pioneering theorists in information theory and communications technology established the category’s greater breadth. For example, in his 1961 classic, *An Introduction to Information Theory: Symbols, Signals and Noise*, John Pierce, a California Institute of Technology professor and the inventor of communications satellite technology, expressly relates the physics of information to the identification of styles in art.²⁰ Music programs sound to create identifiable songs with discrete effects, while painting plots color and texture to create distinct images.²¹

Although we may be accustomed to speaking of such phenomena in more humanistic terms, they are as much modes of organizing relational data as the American Standard Code for Information Interchange (ASCII), the coding system that assigns identifiable symbols to patterns of digital bits. As Pierce observes, art, like telephony or radio, involves the transmission of distinct messages through communications media.²² In the same way a telecommunications engineer seeks to maintain the integrity of a spoken message as it travels through the wires or the airways, composers and painters leverage the dynamics of information processing to create distinct artistic forms. Both the artist and the engineer strive to maximize the efficiency of their respective encoding so as to enable the recipient of the message to identify the source and to perceive discrete patterns.²³

This broadened perspective on information technology similarly pervades the work of Marshall McLuhan, arguably the most influential

17. See generally CLAUDE E. SHANNON & WARREN WEAVER, *THE MATHEMATICAL THEORY OF COMMUNICATION* (paperback ed. 1998).

18. See JOHN R. PIERCE, *AN INTRODUCTION TO INFORMATION THEORY: SYMBOLS, SIGNALS & NOISE* 107-24 (2d rev. ed. Dover Publications 1980) (1961).

19. LLOYD, *supra* note 8, at 13.

20. PIERCE, *supra* note 18, at 250-67.

21. *Id.* at 252-53, 264-66.

22. *Id.* at 264-65.

23. See *id.* at 267.

theorist of the information age. As McLuhan observes, technology programs how people relate to their environment—it is, in short, a *techné*, or craft, in the fullest sense of the word, shaping not just the material out of which it is fashioned, but the users themselves.²⁴ While McLuhan is now best known for his observations regarding electronic media, his own work extends beyond it to examine how a wide range of technologies affect information processing, from the effect of clocks on our organization of time to the role of print in structuring both our physical and social environments.²⁵

Digital media and other modes of information processing are not, however, analogous in all respects. The logic of computer programming is binary; it reduces information to unambiguous alternatives, commonly represented as ones and zeroes. As Lloyd notes, for the modern computer, “ambiguity is a bug”; a statement capable of sustaining multiple interpretations will trigger an error message.²⁶ In contrast, human communication in all its forms is rife with ambiguity—sometimes a cigar is sexually suggestive, and sometimes it is just a cigar.

Far from being an aberration, this aspect of human patterns of interaction actually reflects the complexity evident at the most fundamental levels of existence. Quantum states are not susceptible to description in absolute binary terms; rather than being a one or a zero, the spin and location of a quantum object can be described as exhibiting multiple contradictory values at once.²⁷ In other words, where classical physics would hold that an object “must always be in one state or another, on or off, left or right,” quantum information describes particles in terms of “an ambiguous superposition of two states.”²⁸

To assert that human language and culture exhibit all the traits of quantum behavior extends the analogy farther than current research would support. Nonetheless, superposition serves as an apt metaphor for describing the complexity of information in human cultural communications media. Just as Schrödinger’s cat can be described as both alive and dead before the observer lifts the lid to see what’s in the box, cultural artifacts are capable of supporting an array of contradictory meanings, with different observers perceiving different values.

This systemic complexity has any number of implications for

24. See MARSHALL MCLUHAN, UNDERSTANDING MEDIA: THE EXTENSIONS OF MAN 12-14, 19-20 (W. Terrence Gordon, ed., critical ed., Gingko Press 2003) (1964).

25. See generally *id.*

26. LLOYD, *supra* note 8, at 27.

27. See SEIFE, *supra* note 11, at 182.

28. *Id.*

maintaining the integrity of information across various media. In certain contexts, such as the regulation of automobile traffic, society employs the law to resolve ambiguities in favor of clear discrete values: stop or go, one-way or two-way, no right turn. Other media, however, may actually depend on a degree of ambiguity in order to maintain their integrity. In the example of propaganda, an artistic work may affirm the values of the state, but by failing to accommodate diverse perspectives it can lose its value as a creative work.

Within this environment, law and social norms play a critical role in maintaining the integrity of transmitted messages. Corporate law, for instance, provides various matrices and markers for encoding relations within associative enterprises, balancing the value of enforcing the integrity of signals regarding the allocation of profits and the assumption of risk with the perceived adaptive benefits of free association. Intellectual property performs a similar function; whereas unfettered copying in an unregulated marketplace can obscure critical information as to a product's source, quality and social meaning, the limits on reproduction encoded within an intellectual property system can serve to strengthen the integrity of creative content and identifying symbols.

II. WEAVING TALES AND SPINNING YARNS: A HISTORICAL PERSPECTIVE

Although electronic media may dominate popular discussions of information technology, fashion has played a central role in human communication for upwards of a hundred thousand years. As archaeologists have recently discovered in a series of excavations, ancient jewelry—shell beads with holes used to string them together—provided the earliest evidence of human symbolic thought.²⁹ Not only do the beads themselves demonstrate a capacity for symbolic manipulation and creative gestures, but, researchers observe, the existence of communicative decorations implies the existence of spoken language sufficient to describe them:

“Personal ornaments are a powerful tool of communication,” says Francesco D’Errico at the Institute of the Prehistory and Geology of the Quaternary in Talence, France “They can indicate social or marital status, for example. But you need to have a complex system of language behind that. To me [these beads] are very powerful archaeological evidence that these people were able to speak like us.”³⁰

29. Anna Gosline, *Ancient Beads Imply Culture Older Than We Thought*, NEW SCIENTIST, June 22, 2006, <http://www.newscientist.com/channel/being-human/dn9392-ancient-beads-imply-culture-older-than-we-thought.html> (last visited Nov. 11, 2008).

30. *Id.*

Further reinforcing the symbolic significance of early jewelry are discoveries of beads at sites a considerable distance from water.³¹ The earliest objects known to be exchanged in trade, these prehistoric beads conveyed information that went beyond personal status to the embodiment of relative value.³² In addition, bead discoveries from 75,000 years ago bear the marks of ochre, evidence of ornamental body pigmentation, or prehistoric makeup.³³ The significance of this goes beyond signaling status and relative value to a revolutionary development in personal identity: pride in the creation of a distinct transformative appearance.³⁴

The importance of fashion in defining personal and social identity is equally apparent in early human myths. For example, the creation story that opens the Genesis narrative in the Hebrew Bible uses clothing to symbolize the emergence of human self-awareness. Before Adam and Eve tasted the forbidden fruit, they were naked; after “the eyes of both were opened,” they “sewed fig leaves together and made themselves aprons,” an act that at once communicated their newfound awareness of being more than animals and their act of disobedience.³⁵ The Genesis story also depicts God using clothes as a means of communicating his ongoing protective relation to human beings, despite their disobedience. After imposing punishment, “the Lord God made for Adam and for his wife garments of skins, and clothed them.”³⁶

Greek mythology also provides telling depictions of weaving as an information technology as central to communication as verbal narrative. Homer’s *Odyssey* portrays Odysseus and his wife Penelope in counterpoint, with Odysseus spinning clever tales throughout his journey home while Penelope keeps her parasitic suitors at bay by weaving and unweaving a shroud.³⁷ For the ancient Greeks, the fiber arts were an extension of symbolic thought, as vital to a meaningful existence as speech.

Similarly Odysseus’ guide, Athena, was the goddess of both wisdom and weaving.³⁸ In one of her defining stories, Athena engages in a contest with her devotee Arachne, each using her woven creation to depict signal

31. *See id.*

32. *Id.*

33. Hazel Muir, *Ancient Shell Jewelry Hints at Language*, NEW SCIENTIST, Apr. 16, 2004, <http://www.newscientist.com/article.ns?id=dn4892> (last visited Nov. 11, 2008).

34. *Id.*

35. *Genesis* 3:7 (Revised Standard Version).

36. *Genesis* 3:21 (Revised Standard Version).

37. HOMER, *THE ODYSSEY passim* (Robert Fagles trans., Penguin Books 1996).

38. Susan Ackerman, *Asherah, The West Semitic Goddess of Spinning and Weaving?*, 67 J. NEAR E. STUD. 1, 4-7 (2008).

moments in divine and human history.³⁹ Athena's weaving portrays her role in the creation of her namesake city, Athens, in an image metaphorically illustrating the weaving together of the citizens into a mighty polis.⁴⁰ Arachne, however, uses her weaving to depict the impious acts of the gods, an act which leads to her eventual transformation into a thread-spinning spider.⁴¹

These are, of course, but a few of the mythic narratives worldwide that associate weaving and looms with information. The African spider-god Anansi blends weaving and verbal cleverness into a single form, an amalgam mirrored by the symbolic functions of patterns in kente cloth and other African fabric.⁴² A similar dynamic is evident in Native American mythology, which depicts the weaving of Spider-Woman as the fabric of creation, with textiles as a real-world analogue of the process that shapes the world.⁴³

This association of textiles with communication has continued well past religious myth into the present. In the world of literature, Charles Dickens brought the loom of the ancient Greek Fates into the Victorian era with his archetypal image of Madame Defarge knitting into her needlework the names of those condemned to die.⁴⁴ A contrasting narrative has emerged within the contemporary African American community regarding the role of quilts as information technology encoding the route to safe houses in the Underground Railroad.⁴⁵ Even if this is a modern myth, as some contend, the evident power of the story is itself testimony to the persistence of communal sewing as an icon of social identity.⁴⁶

The significance of textiles and clothing as an information technology encoding personal and social identity has been recognized by select academic theorists as well. In his influential 1964 classic *Understanding Media*, Marshall McLuhan devotes an entire chapter to clothing as a means

39. OVID, *THE METAMORPHOSES OF OVID* 105-09 (David R. Slavitt trans., Johns Hopkins University Press 1994).

40. *Id.* at 107.

41. *Id.* at 107-09.

42. KATHRYN SULLIVAN KRUGER, *WEAVING THE WORD: THE METAPHORICS OF WEAVING AND FEMALE TEXTUAL PRODUCTION* 24-25 (2001).

43. *Id.* at 25.

44. CHARLES DICKENS, *A TALE OF TWO CITIES* *passim* (Grosset & Dunlap 1935) (1859).

45. *See generally* JACQUELINE L. TOBIN & RAYMOND G. DOBARD, *HIDDEN IN PLAIN VIEW: THE SECRET STORY OF QUILTS AND THE UNDERGROUND RAILROAD* (1999).

46. *See* BARBARA BRACKMAN, *FACTS AND FABRICATIONS: UNRAVELING THE HISTORY OF QUILTS AND SLAVERY* 70 (2006).

of processing information.⁴⁷ On one level, he observes, clothing serves as an extension of the skin in regulating our relation to temperature; like a house or office building, clothing extends the information processing in the body's heat-control processes in an external form.⁴⁸ At the same time clothing also serves "as a means of defining the self socially," providing a blueprint for personal and collective values ranging from status and ideology to privacy and connectedness.⁴⁹ While legal scholars—to the extent they acknowledge fashion at all—tend to focus on the role of clothing in signaling one's status as a member of the elite, theorists outside the legal academy have echoed McLuhan in examining the richly diverse ways in which people use fashion as a communications tool.⁵⁰

However, the nature of fashion as an information technology goes beyond the realms of academic theory and cultural narrative. The very origin of modern computing lies in the textile industry—in particular, the invention of programmable punch-card machines to increase the speed and flexibility of luxury silk fabric production.⁵¹ As James Essinger documents in *Jacquard's Web: How a Hand-Loom Led to the Birth of the Information Age*, each card in the loom patented by Joseph-Marie Jacquard in 1804 specified a unit of information pertaining to such critical data as the angle and color of each line of thread, enabling the machine to produce automatically multiple copies of the same design.⁵²

The significance of this invention was not lost on Charles Babbage, the inventor who designed the first modern computer intended for mathematical calculation.⁵³ Babbage studied the Jacquard loom in exacting detail and, as Essinger observes, "really did borrow Jacquard's idea lock, stock, and barrel."⁵⁴ In Babbage's own words when explaining his obsession with Jacquard's work,

You are aware that the system of cards which Jacard [sic] invented are the *means* by which we can communicate to a very ordinary loom orders

47. MCLUHAN, *supra* note 24, at 161-66.

48. *Id.* at 163.

49. *Id.*

50. *E.g.*, MALCOLM BARNARD, *FASHION AS COMMUNICATION* 29 (2d ed. 2002); ROLAND BARTHES, *THE LANGUAGE OF FASHION* 27 (Andy Stafford trans., Berg 2006) (2004); ROLAND BARTHES, *THE FASHION SYSTEM* 59-62 (Matthew Ward & Richard Howard trans., University of California Press 1990) (1967); JEAN BAUDRILLARD, *THE SYSTEM OF OBJECTS* 204-05 (James Benedict, trans., Verso 2d ed. 2005) (1968); FRED DAVIS, *FASHION, CULTURE, AND IDENTITY* 3-8 (1992); ANNE HOLLANDER, *SEEING THROUGH CLOTHES* 311 (1993).

51. *See* ESSINGER, *supra* note 2, at 48.

52. *Id.* at 35-38.

53. *Id.* at 48-49.

54. *Id.* at 47.

to weave *any* pattern that may be desired. Availing myself of the same beautiful invention I have by similar means communicated to my Calculating Engine orders to calculate *any* formula however complicated.⁵⁵

As Babbage himself freely admitted, the key step in the development of the modern computer was the adaptation of information processing in textile production to the processing of abstract mathematical symbols.⁵⁶ Not coincidentally, the language of weaving continues to pervade computerized information processing: from the metaphor of the “web”—mirroring the information arrays embodied in a spider’s silken thread—to the new Weave project of Mozilla Labs.⁵⁷ In fact, contemporary scientific research in the processing of information on a universal scale persists in using the metaphors of strings, knots, and fabric, thereby fashioning mathematical models of the shape of nature that give new life to the divine weavers of ancient myth.⁵⁸ The advent of wearable computing, rejoining the twin progeny of the loom, further underscores this cultural connection.⁵⁹

III. LAYERED LOOK: THE DUAL NATURE OF FASHION AS A COMMUNICATIONS MEDIUM

Creators of fashion are clearly able to weave information into their fabric, but the communicative power of fashion does not end with the author’s text. Instead, fashion is noteworthy for its ability to simultaneously express the point of view of both originator and user. The fashion designer begins by making an artistic statement in the form of a new garment, drawing upon various social and aesthetic forces in order to channel her muse. Then the designer, who may be the equivalent of a celebrated *avant-garde* sculptor or a modest greeting card painter, learns whether her creative vision is also a commercially successful one. The wearer who subsequently acquires the garment gives it dimension and movement, at the same time using the garment to represent her physical body to the world and to broadcast a message about herself, whether deliberately planned or unintended. In other words, every garment potentially functions as an information technology with two concurrent

55. *Id.* (emphasis in original).

56. ESSINGER, *supra* note 2, at 49.

57. Mozilla Labs, *Weave*, <http://labs.mozilla.com/projects/weave/> (last visited Oct. 2, 2008).

58. *See, e.g.*, BRIAN GREENE, *THE FABRIC OF THE COSMOS: SPACE, TIME AND THE TEXTURE OF REALITY* 402-03 (2004).

59. *See generally* ADAM GREENFIELD, *EVERYWARE: THE DAWNING AGE OF UBIQUITOUS COMPUTING* (2006).

messages in superposition: one embodying the designer's authorial voice, and the other generating information on behalf of and about the wearer.

Mainstream American scholars and critics seldom pay much attention to fashion, except perhaps in the context of gender studies, and still less to its communicative functions.⁶⁰ When they do so, their analysis is frequently focused on the consumer rather than on the original designer. Studies of fashion that go beyond technical costume history, moreover, are often heavily influenced by the relationship between clothing and the signaling of socioeconomic status, an association that does not elicit sympathetic treatment from the typical academic.⁶¹ While it is true that the differences between white collar and blue collar uniforms, a luxurious mink and a Republican cloth coat,⁶² or the latest "it" bag and a cheap knockoff offer information about the wearer, such hierarchical indicia are only the crudest measure of identity as expressed by clothing.

Additional data such as specific professional role, group affiliation or disaffection, gender, sexual orientation, moral or religious stance, political perspective, emotional outlook, and aesthetic identity are all manifest in dress—and one need not be a fashionista to recognize the majority of such information. Before an American infant even leaves the hospital, and months before learning to speak, he or she is likely to wear blue or pink clothing, respectively; baby's first code is a dress code. Among adults, consider judicial robes, a New York Yankees t-shirt, a miniskirt, a leather harness over a bare male chest, a yarmulke, a black armband during the Vietnam War, a widow's black veil, or the dark frills of a Japanese Goth Lolita. Each of these garments immediately identifies the wearer to the onlooker, even if the two are complete strangers. Some of these messages are culturally specific: a widow's black veil, for example, is quite anachronistic in modern Western culture and would not scan at all in a society in which the color of mourning is white or in which most women leave the house only if completely shrouded in fabric. Similarly, the wearer of a Yankees t-shirt may be a fan, a girl who borrowed her boyfriend's shirt, or a Bostonian who lost a bet. Such complexity is nevertheless consistent with the function of conveying information.

60. See Valerie Steele, *The F-Word*, LINGUA FRANCA, Apr. 1991, at 18-20. The only fashion journalist ever to receive a Pulitzer Prize for criticism was Robin Givhan of *The Washington Post* in 2006. See The Pulitzer Prizes, Criticism, <http://www.pulitzer.org/bycat/criticism> (last visited Oct. 2, 2008).

61. See, e.g., Jonathan M. Barnett, *Shopping for Gucci on Canal Street: Reflections on Status Consumption, Intellectual Property, and the Incentive Thesis*, 91 VA. L. REV. 1381, 1383, 1386-88, 1388-89 (2005).

62. See President Richard M. Nixon, Checkers Speech (Sept. 23, 1952), available at <http://www.watergate.info/nixon/checkers-speech.shtml> (last visited Nov. 11, 2008).

Within a cultural subgroup, the messages expressed by wearing clothing may be at once more elaborate and harder to translate into words. A dedicated follower of fashion, whose senses are keenly attuned to designer styles, may recognize a kindred spirit via her Manolo Blahnik pumps or his Bape hoodie—articles of apparel that, to the uninitiated, might simply be described as women’s shoes or a sweatshirt, respectively. The inability of one group to recognize all of the signals embedded in another’s toilette, however, no more undermines its expressive function than the insistence of a parent that a teenager’s favorite music is just noise or the child’s retort that all classical compositions sound alike. Some fashion information is directed toward the general public; other information is like a dog whistle or a high-frequency ring tone, audible to certain ears only.

While all clothing communicates information about the wearer, not all wearers are deliberately engaged in crafting an individual aesthetic statement on a daily basis. Much of the time we simply get dressed, in relatively generic garments that resemble those we expect our peers to be wearing. Like a bon mot that eventually becomes a standard phrase or even a cliché, a basic article of apparel like a white button-down shirt is no longer attributable to a particular designer, nor does it communicate a strong, individualized message on behalf of the wearer—though it is not entirely silent, either. Even the least fashion-conscious person, however, is likely to devote extra attention to attire for a special occasion, like her wedding, and to view her choice as a matter of personal expression. As a result, the consumer may be wary of any legal regime that might temporarily restrict her ability to acquire a particular item of clothing, even if the rule’s effect is to enhance the fashion designer’s ability to make creative statements and ultimately provide a wider vocabulary for the wearer.

Clothing is, of course, not the only identity-bearing commodity available to consumers. The choice of a hybrid vehicle over an SUV, a glass of local tap water over a plastic bottle from a distant spring, or a city apartment over a suburban McMansion is dictated by a host of factors, including economic ones, but still expresses the identity of the purchaser. Similarly, a commuter reading the *Wall Street Journal* will offer a different impression than one flipping through a celebrity gossip rag, even though the goal of buying a newspaper is presumably to consume information rather than to generate it. The association between an individual and her clothing, however, makes a particularly strong public statement, since clothing covers the person and represents the individual’s physical being to the world. After all, we may regularly appear without many of our possessions in tow, but we rarely appear without our clothes.

Fashion is a powerful medium of communication, not merely for its creators but also for its wearers. As an information technology, fashion thus functions simultaneously as both message and medium.

IV. A CUTTING-EDGE LEGAL APPROACH TO FASHION AS INFORMATION TECHNOLOGY

The competing messages embedded in fashion foster a systemic regulatory tension, as the law's efforts to protect the integrity of the creator's content may clash with the wearer's choice of personal expression. Similar tensions are inherent in other fields of intellectual property law; in the case of fashion design, however, the current U.S. approach is to ignore the original designer's message to the greatest extent possible and essentially to deny the status of fashion as an information technology. As American fashion enters into a cultural ascendancy and the emerging designer movement brings more individuals into the marketplace as both producers and consumers, pressure is increasing to strengthen legal protection against unauthorized copying—a trend that has prompted complaints against imposing new limits on personal expression.⁶³ The optimal approach to resolving this dilemma is not to view protection or consumption as mutually exclusive absolutes, but to craft a narrowly-tailored statute that respects the complexity of fashion itself.

A. *So Last Season: The Legal Status Quo*

At present, U.S. intellectual property law provides at best partial protection for innovative articles of clothing and accessories. In the absence of comprehensive design protection, the fashion industry has instead over the past century turned to existing areas of intellectual property law that can be extended to some of the individual elements related to a fashion design.⁶⁴

The most widely utilized means of preserving the designer's investment is trademark law, which provides a relatively accessible means

63. See, e.g., Felix Salmon, *Knock-Off Fashion*, <http://www.portfolio.com/views/blogs/market-movers/2007/09/18/knock-off-fashion> (Sept. 18, 2007, 9:38 EDT); Rashmi Ragnath, *Design Protection for Fashion Designs and Autoparts: A Bad Idea Times Two*, <http://www.publicknowledge.org/node/1399> (Feb. 16, 2008, 12:21).

64. For a discussion of fashion designers' efforts over the past century to secure legal protection for their designs, see generally, Susan Scafidi, *Intellectual Property and Fashion Design*, in *INTELLECTUAL PROPERTY AND INFORMATION WEALTH: ISSUES AND PRACTICES IN THE DIGITAL AGE* 115 (Peter K. Yu ed., 2007).

of defending against the incursions of copyists.⁶⁵ Trademarks are, of course, available to almost all goods and services that are exchanged in commerce, including apparel.⁶⁶ Logos and labels, however, are the elements least associated with the design of an individual garment; they are typically affixed late in the design and manufacturing process and do not vary from look to look or season to season.

Because protection for labels and logos is available while protection for the underlying design of a garment is not, the intellectual property regime has a distorting effect on fashion design. The relative availability of trademark protection privileges the display of corporate symbols: the more visible the logo, the greater the item's intellectual property protection, and the better the chance of defeating copyists. As a result, in recent years a number of prominent designers have made the display of logos a prominent feature of their design.⁶⁷ Intensifying the corporate advantage in fashion is the fact that trademark law offers a competitive edge to more established companies with better known brands. If a famous designer is knocked off, consumers may still be willing to pay for the trademarked version. Less familiar emerging designers, by contrast, cannot depend on public recognition to maintain a customer base.

The advantage enjoyed by more established companies is amplified within the narrow category of designs that qualify for "trade dress" protection. This subcategory of trademark law protects not only the usual trademarked symbols, but also product packaging or even product configurations that serve to indicate the source of the goods.⁶⁸ As the Supreme Court opined in *Wal-Mart Stores, Inc. v. Samara Brothers*, product designs like the garments at issue in the case are never "inherently distinctive" or intrinsically capable of source identification.⁶⁹ Instead, the Court held that product designs only point to their origin if they have developed "secondary meaning" in the minds of consumers.⁷⁰ The result is that even without trademark registration, famous designs receive more protection in the form of trade dress than new items on the fashion scene. In the event of design piracy, the owner of a famous design is in a stronger legal position than the emerging designer, and thus more likely to thrive.

65. See 15 U.S.C. §§ 1051-52 (2006); see also 15 U.S.C. § 1125 (2006).

66. See 15 U.S.C. § 1051 (2006).

67. See, e.g., RENATA MOLHO, BEING ARMANI: A BIOGRAPHY 91-92 (Antony Shugaar trans., 2007) (describing designer Giorgio Armani's reluctant decision to incorporate a prominent logo into his Emporio Armani line as a deterrent to copyists).

68. *Wal-Mart Stores, Inc. v. Samara Bros.*, 529 U.S. 205, 209 (2000) (citations omitted).

69. *Id.* at 212.

70. *Id.* at 209-15.

Trademark law is nevertheless far from a panacea, even for designers who have become household names. Fashion trademarks, although protected by law, arguably receive less popular respect than their counterparts in other categories of consumer goods, and articles bearing counterfeit marks are themselves a medium with contested meanings. Shopping for counterfeit fashion is a common vacation activity, both in the U.S. and abroad; New York's Canal Street and Beijing's Silk Market are notorious tourist destinations. Consumers who purchase counterfeit handbags and athletic shoes seek to convey a diverse array of messages, successfully or not. For some, purchasing counterfeits signals their thriftiness and talent for shrewd shopping; others regard counterfeits as an egalitarian challenge to class distinctions; still others believe that their contraband acquisitions are a critique of consumer culture. Congress has not responded to such arguments by creating a trademark exemption for clothing and accessories, however. Rather, it has strengthened trademark protection by enhancing penalties and increasing budgetary support for law enforcement, though the rhetoric supporting such changes has less to do with protection of fashion designers than with fighting organized crime, cutting off funds that might support terrorism, and eliminating child labor.⁷¹

The nature of branding aids in explaining the persistence of trademark protection even in the face of denial of protection for the designs to which labels are attached. In contrast, say, to the shape of a dress, a name or logo is associated with commerce and with the designer as an economic actor. Even when the consumer purchases an item marked with the brand, the designer does not disappear; rather, the product continues to have a visible connection to its source. Maintaining the coherence of the designer's identity is thus an evidently rational act, as justifiable on a visceral level as preventing identity theft. From this perspective, appropriating another's mark conveys a different message, one that is framed primarily by lawlessness and association with unsavory criminal activities.

Like trademarks, patents offer a certain amount of legal protection to fashion, although, given the time, expense, and qualification requirements,

71. See, e.g., Edith Honan, *NYC Campaign Shows Dark Side of Counterfeit Goods*, REUTERS, May 16, 2008, <http://www.reuters.com/article/domesticNews/idUSN1642669920080516>. See generally, e.g., INTERNATIONAL ANTI-COUNTERFEITING COALITION, WHITE PAPER—THE NEGATIVE CONSEQUENCES OF INTERNATIONAL INTELLECTUAL PROPERTY THEFT: ECONOMIC HARM, THREATS TO THE PUBLIC HEALTH AND SAFETY, AND LINKS TO ORGANIZED CRIME AND TERRORIST ORGANIZATIONS (2005), <http://www.iacc.org/resources/resources.php> (follow "IACC White Paper" hyperlink).

to a far lesser extent. A fashion design or design element that is functional can, if deemed sufficiently innovative, be registered as a patentable invention.⁷² Some ornamental rather than functional aspects of clothing and accessories may also qualify for protection through design patents.⁷³ However, as with utility patents, the lengthy process of prior review makes this impractical for most designs due to their seasonal nature. What patent shares with trademark is its focus on an aspect of design relatively separate from the wearer. The elements granted such protections are akin to the characteristic design of a Coke bottle or the functional workings of a hard drive—objects used by the consumer but to a significant degree identifiably distinct.

This quality of separateness also plays a role in copyright protection—not simply in the separability of creative from useful elements required by the useful article doctrine, but in the abiding distinctness of the creative object from the physical form of the wearer.⁷⁴ Jewelry is worn by the consumer, for example, but it has long enjoyed copyright protection as a creative object separable from any underlying function and more akin to a sculpture.⁷⁵ A pendant or bracelet rests on the body relatively unchanged by its wearer and without obscuring or transforming the human shape underneath. Similarly, a print or woven textile design creates a surface pattern akin to a painting or a photograph, an analogy that has contributed to the recognition of full copyright protection for graphic designs emblazoned on shirts and innovative fabric patterns.⁷⁶ Courts have also extended protection to certain distinct artistic features, such as the mask of a Halloween costume, which convey a relatively discrete message apart from their connection to the wearer.⁷⁷

The shape of an article of apparel, by contrast, becomes identified

72. See 35 U.S.C. § 101 (2000).

73. See 35 U.S.C. § 171 (2000).

74. See 1 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 2.08[B][3] (2008) (citations omitted).

75. See *Mazer v. Stein*, 347 U.S. 201, 211-213 (1954); *Trifari, Krussman & Fishel, Inc. v. Charel Co.*, 134 F. Supp. 551, 552-53 (S.D.N.Y. 1955).

76. See *Folio Impressions, Inc. v. Byer California*, 937 F.2d 759, 763 (2d Cir. 1991) (protecting textile design as a “writing”); see also *Eve of Milady v. Impression Bridal, Inc.*, 957 F. Supp. 484, 488-89 (S.D.N.Y. 1997) (qualifying bridal dress lace designs for copyright protection); *Peter Pan Fabrics, Inc. v. Candy Frocks, Inc.*, 187 F. Supp. 334, 336-37 (S.D.N.Y. 1960) (finding copyright infringement of floral pattern textile design). A distorting effect on fashion similar to that of trademark protection also exists in relation to copyrightable elements like fabric prints and embellishment. See *supra* note 66 and accompanying text; Alessandra Ilari, *New Technologies Give Prints Pop*, WWD, Jan. 22, 2008, at 16, available at <http://www.wwd.com/business-news/new-technologies-give-prints-pop-469897>.

77. *Chosun Int'l, Inc. v. Chrisha Creations, Ltd.*, 413 F.3d 324, 329 (2d Cir. 2005).

with the wearer to a more significant degree, such that some may perceive restricting access as an unacceptable limit on self-expression regardless of any harm to the designer. The focus of attention shifts directly to the wearer; to paraphrase art historian Anne Hollander, the design derives social and personal significance from the act of being worn.⁷⁸ Not coincidentally, Congress has thus far failed to extend copyright protection to fashion designs.⁷⁹ The ostensible reason for this exclusion of fashion designs from copyright is that clothing is regarded as merely “utilitarian,” but this is at best an archaic rationalization.⁸⁰ A fashionable consumer does not merely buy any available item of clothing so long as it merely covers enough skin; she chooses the item that appears to make the statement she wants to express. Accordingly, what leads some individuals to resist intellectual property protection for fashion is not a sense that their garments have no creative value, but rather a connection between fashion and identity so strong that they are reluctant to cede the designer ownership of an original creation and control over its availability—unlike the popular acknowledgment of property rights in the author of a novel or the inventor of a better mousetrap. Fashion’s relationship to self-expression, in other words, can prompt selfishness.

The intensity of fashion’s significance as an identity-bearing commodity is reflected in relationships between wearers as well. Despite the fact that nearly all clothing is produced in multiple units rather than as one-of-a-kind pieces, it is still considered a faux pas to appear in the same garment at the same event or in the same context as another person. Nevertheless, the wish for the latest fashion, as opposed to a necessary item of clothing, is often driven by what social theorist René Girard calls “mimetic desire,” or imitation.⁸¹ When a subject desires an object possessed by her model, such as the latest trendy bauble worn by the most popular girl in school or a frequently photographed celebrity, relational conflict may ensue.⁸² The perception of creativity in fashion as limited to the realm of inaccessible luxury goods—an inaccurate but persistent characterization—has the potential to intensify that conflict. In some cases, a consumer’s desire to possess a particular identity-bearing fashion item is subsequently manifest in not only the purchase of a knockoff or counterfeit,

78. HOLLANDER, *supra* note 50, at 451.

79. See H.R. REP. NO. 94-1476, at 55 (1976), *reprinted in* 1976 U.S.C.C.A.N. 5659, 5668 (excluding “ladies’ dress” from protection under the Copyright Act of 1976).

80. *Id.*

81. See RENÉ GIRARD, *EVOLUTION AND CONVERSION: DIALOGUES ON THE ORIGINS OF CULTURE* 56-57 (2007) (defining the “mimetic mechanism,” including mimetic desire).

82. See *id.* at 57, 61-64.

but also in expressions of resentment toward the very fashion house that created the original item of desire in the first place—a form of the scapegoat suggested by Girard's theory.⁸³ The same consumer who implicitly or explicitly acknowledges fashion as a creative medium may thus resist extending a reasonable range of intellectual property protection to fashion, or even respecting those laws already in place, on the strength of desire for unlimited personal expression.

B. Trend Report: Tailoring Law to Fit Creators and Consumers

Despite the partial legal measures adapted to fashion and the piracy perspective of professional copyists and some consumers, circumstances in recent years have changed in ways that render the lack of rational intellectual property protection for fashion designs unsustainable. Advances in technology, globalization of production, democratization of creativity, cultural shifts in America's relationship to fashion, and international harmonization of intellectual property laws all contribute to a need for greater equity in the legal treatment of fashion designs as compared to other creative forms. Since the essence of a well-balanced intellectual property system is to promote creativity, both fashion designers and fashion consumers can benefit from modernization of the current state of the law.⁸⁴

Among the structural changes that have affected fashion designers in recent years are the rise of the Internet and the movement of much fashion manufacturing to nations with low-cost labor forces. While the immediate online availability of photographs of new styles from the runway or the red carpet contributes to consumer interest in cutting-edge fashion, it also enables design pirates to offer fast, cheap knockoffs—often before the original versions are available in stores. Similarly, a copyist who gains access to a trade show can surreptitiously photograph new styles, upload the pictures, send them halfway around the world, and make copies available before the execution of wholesale orders for the original, much less retail sales.

The increase in inexpensive international production following the dismantling of quota systems that had limited U.S. imports of textiles and apparel is a similarly complex development. On the one hand, foreign manufacturing facilitates copying, contributes to the proliferation of sweatshops in countries that do not enforce labor standards, and increases the environmental impact of clothing manufacturing by requiring additional

83. See *id.* at 56, 64-74.

84. See, e.g., U.S. CONST. art. I, § 8, cl. 8.

resources for long-distance shipping; on the other hand, it also enables a creative designer to offer consumers access to original design across price points. Even a consumer who consciously eschews knockoffs can find affordable yet innovative style from a variety of sources: the inexpensive work of emerging designers, the mass-market lines by critically acclaimed designers pioneered by Isaac Mizrahi for Target, and the eponymous diffusion lines of high-end labels such as Giorgio Armani and Ralph Lauren. The infiltration of low-quality, low-priced knockoffs into the market not only limits a designer's ability to recover the investment in the design process through the sale of original works, but also her ability to regulate distribution and to adapt or license the most commercially successful of her more experimental designs for a broader audience. In this environment, a cheap knockoff is not merely a challenge to the designer's business; it undercuts the ability of fashion to serve as an information technology by discouraging the production of designer originals and obscuring the statement made by those who buy the real thing.

An equally important trend is the democratization of fashion design as a creative enterprise. Whether on Etsy, eBay, or in local shops, a new generation of emerging designers has entered the marketplace, most without additional capitalization beyond what they make in their day jobs. As more people attempt to trade on their creative talents, fashion copying takes on a new significance among individuals who might not have otherwise seen it as a problem. Now the concern is not common citizens having access to luxury goods, but the appropriation of designers' personal creativity by corporate design pirates whose stock in trade is the systematic, predatory copying of both famous and unknown individuals' work.

Further destabilizing the lack of protection for fashion design is the effect it has on the integrity of the U.S. government's own anti-counterfeiting message and its commitment to the international harmonization of intellectual property protection. While a counterfeiter who engages in the unauthorized reproduction of trademarks risks both civil and criminal penalties, a design pirate who copies every stitch of a garment except the label is engaged in a legal business practice.⁸⁵ This differential treatment of counterfeiting and design piracy has created a loophole for counterfeiters, some of whom avoid customs enforcement by importing cheap copies that do not yet bear counterfeit labels and then affixing those labels in the U.S.⁸⁶

85. See 15 U.S.C. §§ 1116-18 (2006); 18 U.S.C. § 2320 (2006).

86. Ross Tucker and Liza Casabona, *Making Fakes in the U.S.A.: Counterfeiters Step Up Domestic Manufacturing*, WWD, July 22, 2008, <http://www.wwd.com/fashion-news/making-fakes-in-the-usa-counterfeiters-step-up-domestic-manufacturing-481734>.

Among those nations with influential fashion industries—Paris, London, Milan, and New York host the world’s premier fashion weeks—the U.S. is the only one that does not protect fashion designs. In the E.U. and various countries around the globe, the emerging consensus is to extend protection to fashion designs for a limited period of time, varying between ten and twenty-five years.⁸⁷ With the U.S. exerting pressure on countries such as China to conform to international standards of intellectual property protection, the lacuna in America’s own legal system grows increasingly conspicuous. The signal seems clear: the U.S. wants to shut down copyists in other jurisdictions while allowing its own to thrive.

To adapt to the evolving environment, the U.S. needs to adopt an approach that reflects the complex messages embedded in fashion as an information technology. The wearer’s desire for free self-expression is an important value, but it does not necessarily militate against intellectual property protection for the designer. Unfettered mass copying can increase the noise-to-signal ratio to such a degree that the wearer can no longer achieve her desired effect. Copyists whom the law forces to innovate, moreover, will not simply disappear, any more than newspapers prevented by copyright law from plagiarizing competitors’ articles respond by stopping the presses. Instead, when American law finally rewards fashion innovation rather than imitation, former design pirates are likely to hire young designers and create more choices for consumers. The existence of protection does not hinder consumer self-fashioning through clothing and accessories and may even enhance it; consider that the inexpensive fast-fashion companies that have colonized the globe in recent years, such as H&M and Zara, are European companies in whose home markets copying is prohibited.

At the same time, the advantages accrued from preserving the integrity of the designer’s creative expression may not be sufficient to justify extending protection for the full term of copyright. Fashion is a seasonal medium, and its creators would receive significant relief from protection that applied immediately after the introduction of new designs and during the development or licensing of diffusion lines based on them. In addition, designers may benefit from being able to adapt and/or utilize elements of others’ work that are somewhat more contemporaneous than life plus seventy years old.⁸⁸

87. See Council Regulation 6/2002, 2002 O.J. (L3) 1, 5 (EC); Fusei kyoso boshiho [Unfair Competition Prevention Act], Law No. 47 of 1993, art. 11, *unofficial translation available* <http://www.cas.go.jp/jp/seisaku/hourei/data/u CPA.pdf> (2007). See generally The Designs Act, No. 16 of 2000; INDIA CODE (2000), *unofficial version available* http://www.wipo.int/clea/en/text_html.jsp?lang=EN&id=2398.

88. Cf. 17 U.S.C. § 302(a) (2006) (establishing term of copyright for works published

Rather than maintaining the outdated and unstable status quo, we have an opportunity in fashion to create a model of short-term protection, tailored to the needs of both consumers and creators. The E.U. model offers one alternative, with a short three-year term for unregistered designs or five years for registered designs, renewable for a total of up to twenty-five years.⁸⁹ Another minimalist approach to protection is the term specified in the Design Piracy Prohibition Act, a bill currently under consideration in Congress.⁹⁰ If passed, the Act would protect registered fashion designs for three years, a period that respects the seasonal nature of the fashion industry as well as the inspirational influence of trends.⁹¹ After this brief period of protection expired, a design would enter the public domain.⁹²

The American legal system has too long ignored the importance of fashion design as a complex information technology and has systematically discounted the creative expressions of original fashion designers. From both a theoretical standpoint and a practical one, change is inevitable—and the opportunity to craft a system of legal protection that finally takes into account the perspectives of both creators and consumers is a compelling challenge.

on or after January 1, 1978 as the lifetime of the author plus seventy years after the author's death).

89. Council Regulation 6/2002, 2002 O.J. (L3) 5 (EC).

90. See Design Piracy Prohibition Act, H.R. 2033, 110th Cong. § 2 (2007); *A Bill to Provide Protection for Fashion Design: Hearing Before the Subcomm. on Courts, the Internet, and Intellectual Property of the Comm. on the Judiciary*, 109th Cong. 77-85 (2006) (statement of Susan Scafidi).

91. H.R. 2033 § 2(c)(a)(2).

92. *Id.*



FASHION LAW BOOTCAMP: SPECIAL EDITION
FASHION LAW & TECHNOLOGY

Thursday, July 27, 2017

**Driving and Disrupting the Industry:
Effects of Technology on the Law and Business of Fashion**

Readings

Legal and ethical challenges of production technologies:

Elizabeth Paton, *Fashion That Gets Under the Skin*, New York Times, July 19, 2016, <http://www.nytimes.com/2016/07/19/fashion/leather-dna-alexander-mcqueen.html?contentCollection=weekendreads&action=click&pgtype=Homepage&clickSource=story-heading&module=c-column-middle-span-region®ion=c-column-middle-span-region&WT.nav=c-column-middle-span-region>.

Andy Eckardt, *Adidas Shifts Production - But Robots Get the Jobs*, NBC News, May 25, 2016, <http://www.nbcnews.com/business/business-news/adidas-pulls-back-asia-robots-get-jobs-n579991>.

Ben Ames, *Retailers Sharpen Supply Chain Visibility with Improved Technology*, DC Velocity, April 20, 2016, <http://www.dcvelocity.com/articles/20160420-retailers-sharpen-supply-chain-visibility-with-improved-technology/>.

A Monstrous Mess: Toxic Water Pollution in China, Greenpeace, January 13, 2014, <http://www.greenpeace.org/international/en/news/features/A-Monstrous-Mess-toxic-water-pollution-in-China/>.

Adam Matthews, *The Environmental Crisis in Your Closet*, Newsweek, August 13, 2015, <http://www.newsweek.com/2015/08/21/environmental-crisis-your-closet-362409.html>.

Transforming the Retail Supply Chain: Apparel, Fashion, and Footwear, GS1, http://www.gs1.org/sites/default/files/gs1_apparel_brochure.pdf.

Fashion Transparency Index, Fashion Revolution, April 2016, http://fashionrevolution.org/wp-content/uploads/2016/04/FR_FashionTransparencyIndex.pdf.

Compliance is Not Enough: Best Practices in Responding to The California Transparency in Supply Chains Act, Verite, 2011, http://www.verite.org/sites/default/files/VTE_WhitePaper_California_Bill657FINAL5.pdf.

Sourcemap Selected for Next Generation Higg Index, Sourcemap, January 24, 2017, <http://www.sourcemap.com/blog/2017/1/24/sourcemap-selected-for-next-generation-higg-index>.

Collin Thompson, *How Does the Blockchain Work (for Dummies) Explained Simply*, Medium, October 2, 2016, <https://medium.com/the-intrepid-review/how-does-the-blockchain-work-for-dummies-explained-simply-9f94d386e093>.

Blockchains Smart Contracts: Driving the Next Wave of Innovation Across Supply Chains, Cognizant, June 2016, <https://www.cognizant.com/whitepapers/blockchains-smart-contracts-driving-the-next-wave-of-innovation-across-manufacturing-value-chains-codex2113.pdf>.

Casey Hall, *Indie Brand Babyghost Gets Techie with Scannable Clothes*, WWD, January 11, 2017, <http://wwd.com/business-news/technology/indie-brand-babyghost-gets-techie-with-scannable-clothes-10744841/>.

Retail, start-ups, and the business of fashion itself as a design problem:

Ari Bloom, *To Build Successful Businesses, Start Solving Problems*, The Business of Fashion, June 28, 2016, <https://www.businessoffashion.com/articles/opinion/op-ed-to-build-successful-businesses-start-solving-problems>.

Carey Dunne, *Demystifying Fashion Labs: How Tech Is Changing the Way We Dress and Shop*, Fast Code Design, July 16, 2014, <http://www.fastcodesign.com/3033102/demystifying-fashion-labs-how-tech-is-changing-the-way-we-dress-and-shop>.

Lindsey Thomas, *Introducing Bespoke*, October 10, 2014, <http://www.westfieldlabs.com/blog/introducing-bespoke>.

Chavie Lieber, *Can Everlane Really Become the Next J. Crew?*, Racked, October 8, 2015, <http://www.racked.com/2015/10/8/9442455/everlane-expansion>.

Lauren Sherman, *Is There Still Hope for Fashion Crowdfunding?*, The Business of Fashion, November 26, 2015, <https://www.businessoffashion.com/articles/intelligence/is-there-still-hope-for-fashion-crowdfunding>.

Ruth Simon, *New Rules Give Startups Access to Main Street Investors*, Wall Street Journal, May 11, 2016, <http://www.wsj.com/articles/new-rules-give-startups-access-to-main-street-investors-1462995761>.

Regulation Crowdfunding: A Small Entity Compliance Guide for Issuers, May 13, 2016, <https://www.sec.gov/info/smallbus/secg/rccomplianceguide-051316.htm#3>.

Regulatory frontiers in customer data privacy, retail security, and consumer health & safety:

Claire Swedberg, *Retailer Uses RFID, Cameras, and Social Media to Track Shopper Behavior*, RFID Journal, March 18, 2016, <http://www.rfidjournal.com/articles/view?14214>.

Laura Indvik, *Why Luxury Brands Are Putting Microchips in Your Clothes and Accessories*, Fashionista, April 14, 2016, <http://fashionista.com/2016/04/moncler-ferragamo-rfid-counterfeiting>.

RFID Privacy Policy, Burberry.com, <https://us.burberry.com/legal-cookies/privacy-policy/rfid/>.

Privacy Trade-Offs in Retail Tracking, Federal Trade Commission, April 2015, <https://www.ftc.gov/news-events/blogs/techftc/2015/04/privacy-trade-offs-retail-tracking>.

Katherine Britton, *IoT Big Data: Consumer Wearables, Data Privacy, and Security*, Landslide, November-December 2015, <http://www.americanbar.org/publications/landslide/2015-16/november-december/IoT-Big-Data-Consumer-Wearables-Data-Privacy-Security.html>.

Peeling Back the Apple Watch: Do HIPAA and the Apple Watch Go Together?, Health eSource, September 2015-16, http://www.americanbar.org/publications/aba_health_esource/2015-2016/september/applewatch.html.

Elizabeth A. Harris *et al.*, *Neiman Marcus Data Breach Worse Than First Said*, New York Times, January 23, 2014, <http://www.nytimes.com/2014/01/24/business/neiman-marcus-breach-affected-1-1-million-cards.html>.

Prepared Statement of the Federal Trade Commission on Data Breach on the Rise: Protecting Personal Information from Harm, Committee on Homeland Security and Governmental Affairs, U.S. Senate, April 2, 2014, https://www.ftc.gov/system/files/documents/public_statements/296011/140402datasecurity.pdf.

Alissa M. Dolan, *Data Security and Breach Notification Legislation: Selected Legal Issues*, Congressional Research Service, December 28, 2015.

Connect2HealthFCC: Ingestibles, Wearables, and Embeddables , Federal Communications Commission, <https://www.fcc.gov/general/ingestibles-wearables-and-embeddables>.

Radiation and Your Health: Wearable Computers and Wearable Technology, Centers for Disease Control and Prevention, <https://www.cdc.gov/nceh/radiation/wearable.html>.

Warning Letters Highlight Differences Between Cosmetics and Medical Devices, Food and Drug Administration, <https://www.fda.gov/cosmetics/complianceenforcement/warningletters/ucm081141.htm>.

Green Paper: Fostering the Advancement of the Internet of Things, Department of Commerce, January 12, 2017, <https://www.ntia.doc.gov/other-publication/2017/green-paper-fostering-advancement-internet-things>.

Marketing, social media, and the regulation of social commerce:

The FTC's Endorsement Guides: What People Are Asking, Federal Trade Commission, https://www.ftc.gov/system/files/documents/plain-language/pdf-0205-endorsement-guides-faqs_0.pdf.

Re: Cole Haan, FTC File No. 142-3041, Federal Trade Commission, March 20, 2014, https://www.ftc.gov/system/files/documents/closing_letters/cole-haan-inc./140320colehaanclosingletter.pdf.

Lord and Taylor Settles FTC Charges It Deceived Consumers Through Paid Article in an Online Fashion Magazine and Paid Instagram Posts by 50 "Fashion Influencers," Federal Trade Commission, March 15, 2016, <https://www.ftc.gov/news-events/press-releases/2016/03/lord-taylor-settles-ftc-charges-it-deceived-consumers-through>. (Complaint with exhibits attached)

L'Oreal Settles FTC Charges Alleging Deceptive Advertising for Anti-Aging Cosmetics, Federal Trade Commission, June 30, 2014, <https://www.ftc.gov/news-events/press-releases/2014/06/loreal-settles-ftc-charges-alleging-deceptive-advertising-anti>.

Guides Concerning the Use of Endorsements and Testimonials in Advertising, Federal Trade Commission, <https://www.ftc.gov/sites/default/files/attachments/press-releases/ftc-publishes-final-guides-governing-endorsements-testimonials/091005revisedendorsementguides.pdf>.

Alexandra Steigrad, *FTC Issue Warnings to 45 Celebrities Over Unclear Instagram Posts*, WWD, May 8, 2017, <http://wwd.com/business-news/media/ftc-issued-warnings-to-45-celebrities-over-unclear-instagram-posts-10883342/>.

FTC Staff Reminds Influencers and Brands to Clearly Disclose Relationship, Federal Trade Commission, April 19, 2017 (with sample warning letters to marketers and influencers), <https://www.ftc.gov/news-events/press-releases/2017/04/ftc-staff-reminds-influencers-brands-clearly-disclose>.

E-commerce and authenticity issues, in primary and secondary markets:

Molly Wood and Eliza Mills, *Online Consignment Changes the Game for Used Goods*, Marketplace, December 2, 2015, <http://www.marketplace.org/2015/12/02/business/online-consignment-changes-game-used-goods>.

The RealReal company overview (provided by Nathalie Seufferlein, Sr. Manager, PR & Corporate Communications).

Authenticity, The RealReal, <https://www.therealreal.com/authenticity>.

Ari Levy, *Amazon's Chinese Counterfeit Problem is Getting Worse*, CNBC, July 8, 2016, <http://www.cnbc.com/2016/07/08/amazons-chinese-counterfeit-problem-is-getting-worse.html>.

Timothy Holbrook, *How 3-D Printing Threatens Our Patent System*, Scientific American, January 6, 2016, <http://www.scientificamerican.com/article/how-3-d-printing-threatens-our-patent-system1/>.

Dinusha Mendis et al., *A Legal and Empirical Study into the Intellectual Property Implications of 3-D Printing*, Intellectual Property Office (UK), March 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/421543/A_Legal_and_Empirical_Study_into_the_Intellectual_Property_Implications_of_3D_Printing_-_Exec_Summary_-_Web.pdf.

Seven Best Practices for Fighting Counterfeit Sales Online, MarkMonitor, https://www.markmonitor.com/download/wp/wp-Fighting_Counterfeit_Sales.pdf.

Anna Stec et al., *Textile Counterfeiting DNA to Improve Supply Chain Integrity*, Advanced Textile Source, September 18, 2015, <http://advancedtextilesource.com/2015/09/textile-counterfeiting-dna-to-improve-supply-chain-integrity/>.

FASHION & STYLE

Fashion That Gets Under the Skin

On the Runway

By ELIZABETH PATON JULY 19, 2016

LONDON — When it comes to fashion, how far would you go to show your appreciation of your favorite celebrity?

Millions of fans choose to dress like their idols. Others buy outfits from the multitude of clothing lines or cosmetic ranges endorsed or designed by Hollywood stars. But would you — could you — ever wear a leather jacket or carry a handbag containing their DNA?

The Central Saint Martins graduate Tina Gorjanc believes that advances in tissue-engineering technology could create a highly lucrative and hitherto untapped niche within the luxury market. Last month, she unveiled Pure Human, a range of leather prototypes that she theorizes could be grown from DNA extracted from hair samples of the fashion designer Alexander McQueen.

“Pure Human is a critical design project that also highlights the major legal loopholes around the protection of biological information, particularly in Great Britain,” Ms. Gorjanc said at her end-of-year show.

The 26-year-old, originally from Slovenia, was standing near her mock-up collection of stylish biker jackets and totes, at this stage made out of pigskin. The flesh-toned pieces bore freckles, sunburn and tattoo etchings that matched those once found on Mr. McQueen’s body. A lock of his hair, which came from strands that Mr. McQueen had sewn into items in his 1992 Central Saint Martins graduate

collection, entitled “Jack the Ripper Stalks His Victims,” and skinlike samples from earlier laboratory tests were encased in glass cabinets close by.

Though Ms. Gorjanc cannot patent Mr. McQueen’s DNA itself, she can apply to patent his genetic information samples as the source for a procedure that would result in laboratory-grown leather made from human tissue. This involves taking Mr. McQueen’s DNA from a hair sample, then transplanting it into stem cells and then multiplying those cells.

She filed that application in May and is now applying for a second patent, this time for the process of extraction itself (not source-dependent) to bolster the future development of the project.

“If a student like me was able to patent a material extracted from Alexander McQueen’s biological information, and there was no legislation to stop me, we can only imagine what big corporations with bigger funding are going to be capable of doing in the future,” Ms. Gorjanc said.

She added that the Human Tissue Act, passed in Britain in 2004, which regulates the removal, storage and use of bodily tissue, currently relates to the handling of human genetic materials for medical but not commercial purposes.

Kering, the French luxury group that owns the Alexander McQueen brand, is “aware of the project,” with several McQueen employees coming to see the presentation at the Central Saint Martins campus in Kings Cross, Ms. Gorjanc said. According to an Alexander McQueen spokesman, “Alexander McQueen was not approached by the designer about this project and we do not endorse it.”

Friends and former employees of Mr. McQueen, who committed suicide in 2010, told Ms. Gorjanc that the project was the sort of provocative experimentation he would have enjoyed and encouraged.

“I know many people have been made uncomfortable by the work I’ve been doing, calling it Frankenfashion, but I think I am prompting the right sort of questions for this industry in the 21st century,” Ms. Gorjanc said. “The demand for personalized and unique, rarefied product is only getting greater and greater. So is

obsession with celebrity, not to mention advances in biotechnology, could change the way we manufacture garments and their fabrics forever.”

Ms. Gorjanc pointed to the Brooklyn-based company Modern Meadow, which “grows” biofabricated leather in labs from collagen proteins found in living cells, bypassing animal slaughter in a bid to create a more sustainable supply chain, as an example of the growing convergence between biotechnology and the fashion world.

Modern Meadow recently raised \$40 million in another round of funding as it seeks to become a top source of leather for the world’s largest accessories houses. But at this stage, Ms. Gorjanc said that no part of the Pure Human project is for sale (not least because her patent applications are still pending).

“Eventually perhaps this showcased range could go into a gallery, or hands of collectors, but they aren’t intended for commercial use,” she said. “At this stage, they are purely to promote the possible application of the technology. The purpose of using Alexander McQueen’s genetic information in my patent is to show that the products made from using him as a source — or indeed from anyone — can be patented in the first place.”

According to Hugh Devlin, a partner at the law firm Withers Worldwide in London who specializes in advising brands in the fashion and luxury sector, such genetic design work could run into problems within Britain on public morality grounds, or if donors did not give informed consent for the use of their cells.

“One of the issues with living in a country like the U.K. is that the courts can step in to opine in the event that existing legislation has not addressed something,” he wrote in an email, adding that there could also be trademark issues if Ms. Gorjanc were to try to use the name of the source of the cells as a marketing element.

In Britain, and more widely in Europe, the European Union Tissue and Cells Directives was set up to establish a joint approach to the regulation of tissues and cells across the Continent.

But in the United States, existing legislation and court precedent are

inconsistent when it comes to the issue of profit from human body product. Any ownership you may have in your tissues vanishes when they are removed from your body, with or without consent, despite a raging battle among scientists, lawyers, disgruntled patients and their families.

But the Federal Policy for the Protection of Human Subjects, a.k.a. the Common Rule, requires that scientists tell research participants that they can withdraw from a study at any time without penalty (this does not help, obviously, with anyone who is dead).

As it happens, Ms. Gorjanc's is not the first apparent fashion initiative at the intersection of trend-based luxury and biology. Human Leather, a British-based company, claims to create products from donated human skin "for a small but highly discerning clientele," with prices ranging from 9,000 euros (\$9,950) for a wallet to 18,000 euros for a pair of shoes. But given that the website registrant is anonymous, there are allegations that the site may be a hoax. Ms. Gorjanc, however, is not joking.

Correction: July 20, 2016

An earlier version of this article described incorrectly how Modern Meadow develops cultured leather products. It biofabricates leather from collagen protein and other essential building blocks found in animal skin. The company does not use animal cells. *Continue following our fashion and lifestyle coverage on Facebook (Styles and Modern Love), Twitter (Styles, Fashion and Weddings) and Instagram.*

A version of this article appears in print on July 24, 2016, on page ST10 of the New York edition with the headline: Delving Into a DNA-Infused Fashion Niche.

MAY 25 2016

Adidas Shifts Production — But Robots Get the Jobs

by ANDY ECKARDT

MAINZ, Germany — Adidas is relocating some of its shoe production from Asia to the company's homeland — but Germans shouldn't expect a jobs boom.



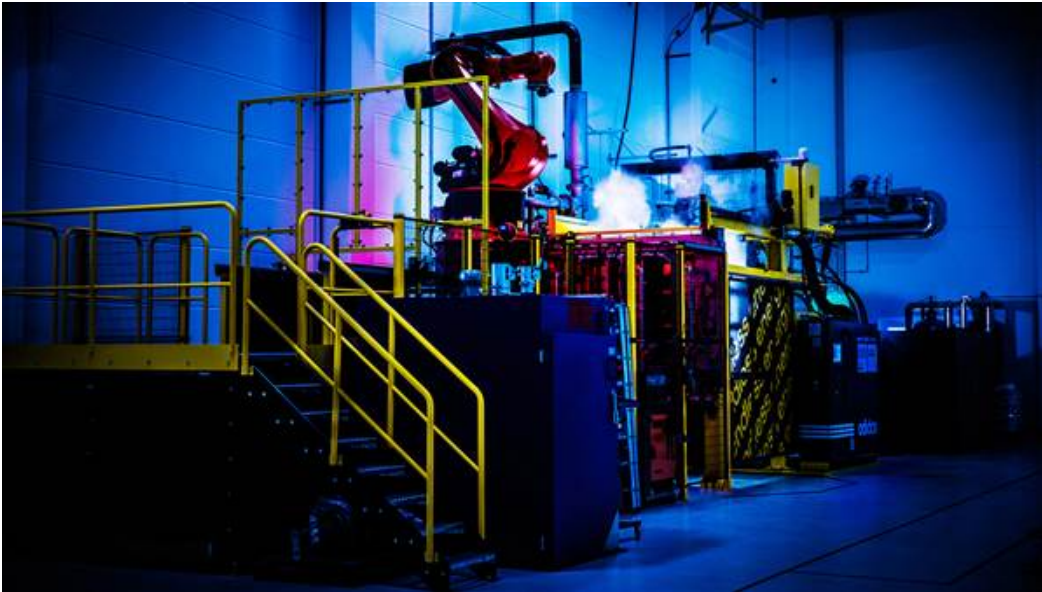
Adidas shoes worn by U.S. runner Jeremy Wariner during the AA Drink FBK Games in Hengelo, Netherlands, on May 22. Dean Mouhtaropoulos / Getty Images

What is currently done by hand will soon be carried out by robots as part of what the firm calls an "automated revolution."

The sportswear giant unveiled its prototype "Speedfactory" on Tuesday — a 3,000-square-foot, high-tech facility in the southern German town of Ansbach.

The first 500 robot-made high-performance running shoes are scheduled to be rolled out later this year.

"We believe that this is pioneer work for a fully automated production process," Adidas spokesman Jan Runau told NBC News, adding that the facility will mean the firm "will be able to get the desired product to the customer much faster."



Adidas unveiled a prototype of a "Speedfactory" in Ansbach, Germany, on Tuesday. Adidas

Adidas moved its production to Asia in the early 1990s, mainly due to rising wage costs in Europe. It kept just one production facility open in Germany, where 700,000 soccer shoes are produced annually.

Overall, Adidas manufactures more than 300 million sports shoes per year. The firm initially plans to produce around 1 million shoes in Germany.

A 50,000-square-foot "Speedfactory" is due to be finished in Ansbach by the end of 2016. A second is expected to open in the U.S. next year while a third is also in the pipeline, according to Adidas.

TECHNOLOGY April 20, 2016

STRATEGIC INSIGHT | VISIBILITY & CONTROL

Retailers sharpen supply chain visibility with improved technology



To meet the challenge of rising e-commerce sales, businesses are pushing visibility beyond their own warehouses, to include suppliers, partners, and goods in transit.

By **Ben Ames**

E-commerce as a proportion of total retail sales is growing fast, and that constantly changing landscape is forcing many retailers to seek tighter control over their inventory levels and deployment. In order to keep up with the quick fluctuations of online commerce, retailers need precise visibility over their goods at all times.

Now, leading retailers have found a promising solution, as improved technology allows them to track every item in their inventory, whether it sits in their own warehouse, in a supplier's factory, in a partner's DC, or even in a tractor-trailer or shipping container.

This level of precise visibility leverages improvements in computing, sensors, storage, and big data. The result is important to retailers because it allows them for the first time to react to changing market conditions in near real time.

VISIBILITY IS CRUCIAL IN E-COMMERCE

Although U.S. e-commerce sales in 2015 accounted for just 7.3 percent of the nation's total retail sales, that picture is changing fast, [U.S. Census figures show](#). E-commerce sales grew 14.6 percent over 2014's figures, to \$341.7 billion, compared with growth of just 1.4 percent for total retail sales.

Much of the pressure to improve visibility throughout the supply chain comes from that explosive growth of e-commerce, which is more sensitive to market fluctuations than traditional in-store sales. Online markets can explode or collapse seemingly overnight in response to triggers like weather, fashion, current events, or social media.

Supply chain visibility is one of the crucial capabilities a company must master in order to respond to those swiftly changing conditions, according to "[Keeping Up with the Retail Consumer: 6 Supply Chain Disciplines Retailers Must Master](#)," a 2015 market study by Adelante SCM and Legacy Supply Chain Services.

The study defines supply chain visibility as "having timely, accurate, and complete data and information related to orders, shipments, inventory, sales, costs, assets, and other supply chain-related items."

That may sound like a tall order, but for companies that can achieve it, the rewards are vast. Armed with sharper visibility, retailers can better answer daily questions about order status, shipment location, inventory counts, and forecast accuracy, the study says.

To reach that goal, most companies must overcome challenges such as data stuck in silos, infrequent batch communications, low-tech shipping processes, and frequently changing trading partners, the report concludes.

SHINING A LIGHT ON "BLACK HOLES"

For many years, those hurdles were too high for the average retailer to clear, but recent technology advances have given them a boost, says Jim Hayden, vice president of solutions at Savi Technology Inc. Data can finally flow freely and swiftly among the links in a supply chain thanks to cheaper computing and data storage, along with sensors that boast greater transmission range and longer battery endurance.

Those devices permit users to constantly monitor the status of each shipment, instead of waiting for drivers or dock workers to check a shipment in when it arrives at a terminal or crosses a border, as had long been the case.

"What we've seen in the supply chain is that the definition of visibility is milestone-based—just asking, 'Was it picked up from the factory?' or 'Has it arrived at the warehouse?'" Hayden said. "But there was nothing in between, so that was a black hole."

But that's all changing. Retailers with sharper visibility can finally peer inside those black holes and see exactly where they need to tweak their processes in response to changing market conditions.

Armed with granular data about the movement of goods, both shippers and receivers can make adjustments while the goods are still in transit. For instance, a company could delay a manufacturing shift if a shipment of supplies is going to be late, or hold a departing delivery truck until a cross-docked item arrives at the DC. This strategy also enables retailers to keep up with the frantic pace and volatile demands of e-commerce. And it provides a crucial tool for retailers engaged in omnichannel operations—that is, taking orders from both stores and online sites and fulfilling those orders from either retail shelves or warehouse racks.

"In an omnichannel world, with the dynamic way orders are coming in, retailers are using different channels to fulfill orders," Hayden says. "That includes extending their warehouses to include goods in transit."

A retailer that can monitor goods in transit can pinpoint each incoming shipment while it is still on the road, allowing the company to react to sudden changes in demand by diverting a truck to a retail store instead of the warehouse for which it was originally intended.

BETTER VISIBILITY WITH CONTROL TOWERS

Generating data is key to achieving better visibility, but companies gain the greatest improvements when they translate that data into "actionable planning," says Vikram Balasubramanian, senior vice president of product management at MercuryGate International Inc.

"Visualization itself is not a solution, unless it's tied to the business process it enables," Balasubramanian says. "For the supply chain, it's what you do with it once you gain visibility that matters."

Although many users have expressed interest in a "control tower" to manage their supply chain data flow from a central hub, the term is loosely defined, Balasubramanian said. At the basic level, users simply practice exception management and respond to missed deadlines or late shipments after they occur.

A more advanced version of a control tower provides sharper visibility by empowering users to make decisions earlier, Balasubramanian said. Such a system could, for example, automatically alert a truck driver of oncoming weather and offer him or her an alternative route.

CLOUD COMPUTING OFFERS A CLEAR VIEW

Unlike weather forecasters, supply chain managers say clouds can actually improve their visibility ... cloud-based computing platforms, that is. Instead of hosting a software application or database on servers located in their own buildings, users of cloud-based platforms rely on providers to host the apps remotely and provide access over networks.

Hosting data in the cloud can make it easier for supply chain partners to both provide and access information regardless of where in the world they are located, and thus combine global visibility with

business practice engines such as predictive and prescriptive analytics, says Jim Hoefflin, president and COO of supply chain software developer Kewill.

All of these changes have helped to reduce or eliminate the frequent information gaps that shippers saw just five or 10 years ago, when supply chain visibility was restricted to pickup and delivery milestones, Hoefflin says.

That improved visibility has evolved just in time to help retailers who are under pressure from the increasing complexity of global trade and are keenly aware that a large portion of their inventory is locked up in the supply chain in motion, he says. Applying the tools of advanced visibility allows companies to alter that inventory in process, steering certain shipments to new destinations in reaction to real-time information about changing markets.

What's next in supply chain visibility? While a few top retailers have begun to practice advanced visibility, future improvements could makes it easier for all retailers to extend visibility beyond their corporate walls to include collaboration with supply chain partners and, someday, to see all the steps of shipping, planning, and fulfillment at once.

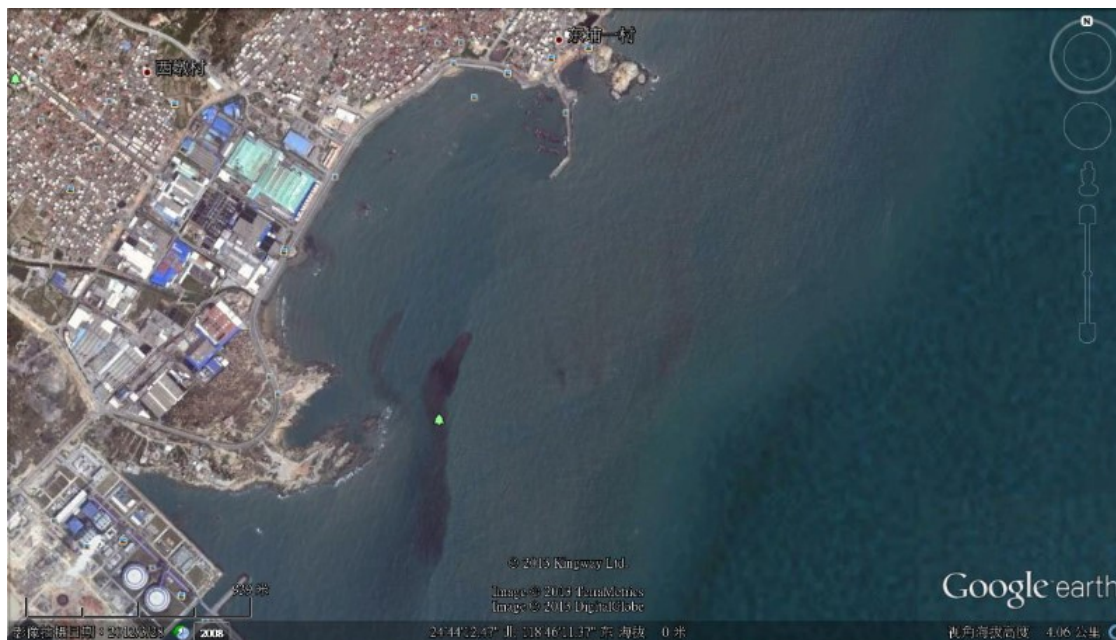


A Monstrous Mess: toxic water pollution in China

Feature story - 23 January, 2014

A team from Greenpeace East Asia's Detox campaign recently discovered an unsettling sight off the coast of South Eastern China. Next to the city of Shishi, a centre for children's clothing production, they discovered a huge black plume of wastewater around the size of 50 Olympic swimming pools on the sea's surface; a large dark scar on the water easily visible via satellite imagery.

[Further research](#) indicated that this plume was coming out of a discharge pipe from the Wubao Dyeing Industrial zone and more specifically, the Haitian Environmental Engineering Co. Ltd wastewater treatment plant which serves 19 of Shishi's textile dyeing facilities.



Following this discovery, Greenpeace activists collected and tested discharge water coming from two of the facilities at the Wubao zone towards the wastewater plant for treatment. The findings were released in a study entitled [A Little Story About a Monstrous Mess II](#). The tests revealed the presence of a range of hazardous chemicals such as the hormone disruptor nonylphenol (NP), chlorinated anilines and antimony in the wastewaters. Despite our attempts to sample the outfall into the sea, it was not possible to access the discharge point underwater.

The toxic water pollution scandal uncovered at Wubao, Shishi is just the tip of the iceberg. In China alone there are 435 discharge points like the one serving Wubao, spanning the coast and releasing 32.2 billion tons of wastewater into the sea each year. In 2012, a staggering 68% of them had records for illegal discharge while 25% had never met national environmental standards, according to [official data from China's state Ocean Administration](#).

Polluting our waterways, contaminating our clothes

Greenpeace East Asia went on to test children's clothing purchased and produced in Shishi and another centre for children's textiles, the city of Zhili in Zhejiang Province. Together, these two cities account for 40% of all the

children's clothes made in China. The [testing revealed](#) that many of the very same chemicals found in the dyeing facilities discharge wastewater were also in the clothes themselves. Greenpeace tested 85 clothing items for a range of hazardous chemicals including phthalates, antimony and nonylphenol ethoxylates (NPEs) which break down to form the toxic chemical nonylphenol (NP). The findings revealed:

- 26 samples tested positive for NPEs with the highest concentration reaching 1,800 mg/kg
- Over 90% of the samples containing polyester tested positive for antimony
- Two samples were found to contain phthalates with a concentration of above 1,000 mg/kg, the highest being 1,7000 mg/kg. It was also found in some other products, though at lower concentrations

Protecting our Little Monsters

The use of hazardous chemicals during the manufacture of children's clothing poses a large-scale problem in China and around the world. Not only is it leading to environmental pollution locally, as seen from the discharges in Wubao, residues of these substances can also be found amongst the millions of products, sold and exported across China and to countries all over the planet from textile towns such as Shishi and Zhili. For example, 70 – 80% of products produced in Shishi are exported to countries in the Middle East, Europe, North America, Southeast Asia and Africa.



The continued use of hazardous chemicals such as these, not just in clothes but also in children's toys and other products, will inevitably lead to increased levels being released into the environment either at the site of production or from various other sources. This can include domestic washing machines or even from some products into the air. Given the scale of manufacture in the textile industry, the use of these chemicals, even at low levels, can lead to considerable amounts ending up in our environment, increasing children's exposure to these hazardous substances and heightening the potential health risks they pose.

Compared to adults, children can be more sensitive to some effects of certain hazardous chemicals. Some chemicals have the ability to interfere with children's normal hormone functions and affect the development of the reproductive system, immune system or nervous system.

The bigger picture

The findings at Zhili and Shishi are just a snapshot of a much larger problem within China's textile industry. In China today there is no adequate regulation to strictly oversee the use of hazardous substances used at the hundreds of production sites such as Shishi. This chemical management regulation is critical to ensuring that hazardous chemicals are no longer used to manufacture clothing and other textiles for children or adults.

Greenpeace is calling on the Chinese government to enforce a crucial new piece of policy that requires factories that use and discharge hazardous chemicals to register and disclose to the public the release and transfer information of hazardous chemicals. In some places like Mexico and Taiwan crucial first steps are being taken towards critical chemical regulation and showing that it can and should be done.



"Two Greenpeace activists submit the findings of the Monstrous Mess II report to China's Ministry of Environmental Protection as an early Chinese New Year gift."

A global problem with a global solution

Government regulation has a key role to play but the textile industry also needs to act with urgency. Greenpeace's global Detox campaign is calling on major brands to take action now towards this shared goal of a toxic-free future. Thanks to global people power well-known brands like [Zara](#) and [Mango](#) are already taking landmark steps towards supply chain transparency – ensuring factories reveal discharge information publicly – and towards elimination of all hazardous chemicals.

However, there is still more work to do. Following on from its report on Chinese textiles, Greenpeace East Asia's [most recent study](#) revealed a range of potentially hazardous chemicals in children's clothes made by leading international clothing brands such as Burberry, Disney and Adidas. While their competitors take credible steps to come clean these brands continue to lag behind.

Tehran Twister / Climate Change: What Would Darwin Do?

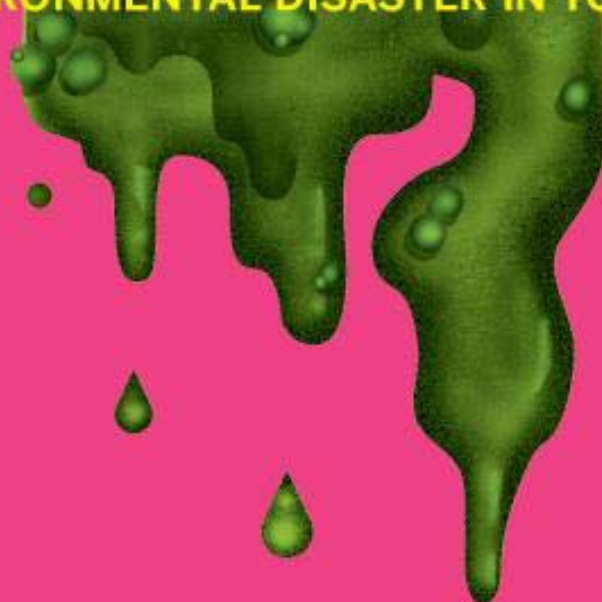
Newsweek

08.21.2015



TOXIC FASHION

THE ENVIRONMENTAL DISASTER IN YOUR CLOSET



The Environmental Crisis in Your Closet

BY ADAM MATTHEWS / AUGUST 13, 2015 11:25 AM EDT

Approach the massive Orathupalayam Dam by road, and it quickly becomes clear that something has gone terribly wrong. Within 2 miles of the dam, the lush rice paddies, coconut palms and banana trees that have characterized this part of southern India suddenly give way to a parched, bright red landscape, dotted only with scrub forest. The Noyyal River, which used to be clean and clear, now runs foamy and green, polluted with the toxic runoff of the titanic textile industry 20 miles to the west, in Tirupur.

At first glance, Tirupur, aka “Knit City,” appears to be an exemplar of how globalization can improve the developing world. The garment industry here in the south Indian state of Tamil Nadu earns billions of dollars annually, employs about a half-million people and exports clothes to Europe and the United States. Chances are good that if you have a Gap, Tommy Hilfiger or Wal-Mart T-shirt marked “Made in India,” it came from here.

American taxpayers have played a key role in turning Tirupur into a manufacturing powerhouse. In 2002, the United States Agency for International Development (USAID) loaned \$25 million to the government of Tamil Nadu and a local clothing industry group, the Tirupur Exporters Association, to finance [a new water-delivery system](#). It kick-started a slew of investment into the project; a local consortium [eventually raised](#) an additional \$220 million. The U.S. consulate in Chennai in a 2006 [press release](#) explained that before the American intervention, the local industry “was running out of water, a critical input for dyeing and bleaching.” As a side note, the release noted that the thousands of slum dwellers in the area could finally have access to treated, running water.

The USAID project, which piped in clean water from a stretch of the Noyyal in a nearby farming region, helped the local industry boom. Between 2002 and 2012, U.S. knitwear imports from India jumped from \$571 million to \$1.25 billion, and [an estimated 56 percent](#) of those garments came from Tirupur. But all that growth has had devastating consequences for the environment and people living in the area.

In early April 2013, I met the leader of the Orathupalayam Farmers Association, Chelliappan Udayakumar, near the Orathupalayam Dam. For generations, Udayakumar’s family farmed this land, growing local crops such as rice, banana, coconut and turmeric. “There were good jobs

and good livelihood,” says Udayakumar. Now, “there is no cultivation of the land, no income.” The small-scale agriculture lifestyle that characterized the region for centuries, he says, has “fully collapsed.”

He walked me through Orathupalayam village, a small town at the base of the dam. Abandoned brick homes painted light blue and topped with red tile roofs dominated the main square. Plaques on the homes commemorated their erection—most date from the late 1980s, when construction of the dam began. Twenty-five years later, the Orathupalayam is one of over 60 villages that have been transformed into ghost towns.

The dam was supposed to update agricultural irrigation practices in Tirupur. But by the mid-2000s, the water was so saturated with chemicals, salts and heavy metals that local farmers were petitioning the Madras High Court—the highest court in Tamil Nadu—to not release the water into their fields. It was making farmland unusable and locals sick. In 2002 and 2003, a local university set up [three camps](#) to examine the health effects of the toxins downstream. In one of the camps, doctors found that about 30 percent of villagers suffered from symptoms—including joint pain, gastritis, problems breathing and ulcers—connected to waterborne diseases. A [2007 study](#) by a local nongovernmental organization found that Tirupur’s 729 dyeing units were flushing 23 million gallons per day of mostly untreated wastewater into the Noyyal River, the majority of which collected in the Orathupalayam Dam reservoir. When officials finally flushed the dam in the mid-2000s, 400 tons of dead fish were found at the bottom.

Comically Corrupt

A couple of weeks after I visited Tirupur, on April 24, 2013, Rana Plaza, an eight-floor complex of clothing factories in Dhaka, Bangladesh, caved in, [burying over 1,100 workers](#) in the rubble. As the dead dominated newscasts, brands like [Wal-Mart Stores Inc.](#) and [United Colors of Benetton](#) momentarily defended their labor and safety records. Activists called for boycotts, and President Barack Obama even [revoked](#) Bangladesh's right to export certain clothing items to the U.S. without paying tariffs.

Rana Plaza resonated with American consumers. After all, even Bangladeshi women earning less than two bucks a day deserved to go to work in the morning confident that they would be alive that evening. But while the disaster did force Westerners to take notice of the plight of those who make their clothes, a larger environmental crisis in the region continued unnoticed—

despite impacting many hundreds of millions of people.

According to Yixiu Wu, who helms Greenpeace's "Detox My Fashion" campaign, the average pair of jeans requires 1,850 gallons of water to process; T-shirts require 715 gallons. And after going through the manufacturing process, all that water often ends up horribly polluted. The textile industry today is the second largest polluter of clean water after agriculture, and it has an outsized effect on the people of Asia.

In large part, that's because over the past two decades American clothing brands have steadily moved production out of the U.S. and into Asia. The American Apparel and Footwear Association estimates its members outsource the manufacturing of 97 percent of their clothing, more than 75 percent of it to Asia. "Simply put: We are a nation of 330 million importers," the trade group says.

The benefit to the U.S. consumer is clear: Just drive to a nearby mall and pop into H&M, Uniqlo, Gap or any other fast-fashion label, and check the clothing tags. It's likely that they'll say the garments were made in Cambodia, Laos, Indonesia, China or Bangladesh—all countries competing to make a T-shirt that costs Americans and Europeans just \$5 but takes a heavy toll on the people at its source. Near critically polluted waters like Bangladesh's River Buriganga and Cambodia's Mekong River, life-sustaining farms are dying, potable water has become toxic and locals are now at great risk for serious illness, all as a result of industrial-scale clothing manufacturing.

At the core of this environmental and health disaster is the poor state of regulatory institutions throughout much of South and East Asia. Transparency International's annual Corruption Perception Index paints a dispiriting picture: Cambodia and Burma (two of the latest hot spots for textile manufacturing) are tied with Zimbabwe at 156 out of 175 countries ranked, while Laos and Bangladesh are tied at 145. India fares a lot better at 86, but even there, human rights and environmental preservation are often trumped by the need to provide a business environment that can compete with more corrupt countries.

In a 2013 study, Indian environmental scholar Geetanjoy Sahu investigated the country's various state pollution control boards, responsible for regulating the environmental impact of all sorts of industries, including clothing manufacturing. Sahu, drawing on data gathered through Right to Information Act requests (similar to the U.S. Freedom of Information Act), found that the boards are often underfunded, understaffed and run by political appointees with no scientific background.

The pollution control boards for two ocean-facing Indian states frequently cited as development models—Tamil Nadu and [Gujarat](#)—are especially corrupt. For example, a [2008 paper](#) by Sahu explains in detail how the Tamil Nadu Pollution Control Board failed to stop the massive spread of pollution from leather tanneries. In February 2015, a wall in a pit holding tannery effluent collapsed, drowning 10 employees in toxic sludge. The plant had been approved by two TNPCB inspectors, who were arrested and jailed for allegedly receiving a bribe of more than [\\$3,000](#) to approve the factory's license. The two men are facing charges in a [local court](#) in Tamil Nadu of three counts of corruption, reckless endangerment, negligence and involuntary manslaughter. A third, more senior, official is also [being investigated](#).

Pamela Ellsworth, chairperson of the Fashion Institute of Technology's [Global Fashion Management Program](#) and a supply chain expert, says the core problem is that people in the U.S. and Europe expect both a low price and a responsible corporation—and the margins clothing companies require often make it difficult for suppliers to meet corporate vendor codes of conduct and still earn a profit. “Eventually we are going to have to train consumers in the U.S. to pay more for clothing,” she says. “It can't be the only commodity that gets cheaper every year.”

Bottled Water Unfit to Drink

In the wake of the Rana Plaza disaster, India's clothing industry has presented itself as the sustainable, safer alternative to Bangladesh. On September 19, 2013, the Tirupur Exporters Association and the Indian Consulate in New York City co-hosted an event in Manhattan's Garment District, a few blocks from the 34th Street fast-fashion strip. The event was designed to attract orders from American clothing brands, and the message was simple: Fiascos like Rana Plaza won't happen in India.

"The Indian apparel industry is compliance-oriented, and we follow all the rules of the game," Arumugam Sakthivel, president of the association, [told the Press Trust of India](#) at the time.

Sinnathamby Prithviraj isn't buying it. The chubby, pompadoured and mustachioed social activist is one of the leading critics of the local clothing industry. He's been fighting for years to publicize—and end—the industry's polluting practices. In 2007, after a decade-long legal battle to shut down dyers who flagrantly violated pollution rules to supply major U.S. brands, Prithviraj and a group of farmers won a decision by the Supreme Court of India to shutter any

dyers who hadn't brought their liquid discharge down to zero. But India's legal system moves slowly. The Dyers Association of Tirupur filed appeal after appeal, and the dyers continued to operate in the interim, despite being in contempt of the court's decision.

Meanwhile, as orders from major brands like Gap and Wal-Mart increased, so did the release of even more toxic wastewater. Then, in 2011, in what seemed like a triumph for the environmentalists, India's Supreme Court told the utility company in Tamil Nadu to cut power to any dyeing factories in contempt of its order. Most of the factories could not afford to conform to the requirements and ended up shutting down.

But this turned out to be a Pyrrhic victory for Prithviraj and his farmers. Wildcat dyers in outlying districts sprang up, and soon Tirupur's garment pollution problem had spread statewide. In Namakkal, an adjacent district where inspectors are engaged in a game of whack-a-mole to shut down illegal dyers, M. Murugan, the pollution control board's local environmental engineer, admits he's fighting a losing battle. "Many units are small, mobile and can function without electricity," he says. Over the past two years, the Namakkal pollution control board has averaged one or two raids per month. "Ultimately, if we demolish [the dyeing industry] in Namakkal, in some other place it will come again," he says.

In April 2013, Prithviraj told me he wasn't sure what to do next. "Although we won the case, practically, we lost it. We don't have the eyes and human resources to watch what's going on illegally." And, he added, India is "a country where anything can be done illegally."

The next day, Prithviraj sent me out with his driver to see just how lawless the industry can be. For about an hour, my photographer and I snooped around a government-run industrial park home to a number of textile factories. But as I was gathering water samples from the river, the photographer strayed across a bridge to take pictures of a nearby factory, which he believed was

illegally discharging waste into the ditch in front of the building. That's when men began to approach us from several directions. I ran to the car to avoid a confrontation; the photographer seemed less concerned and kept snapping shots.

I yelled for him to speed up and get back in our SUV, but he waved me off, strolling leisurely back to the vehicle. A large crowd gathered. A minute later, we were trapped. One of our pursuers, a brawny man in his early 30s with a shaved head and a clean, striped button-down shirt, blocked our car with his body. An older man joined him and produced a card saying he

was from the TNPCB. Our driver, who had seen many such cards, immediately said it was a counterfeit. But the man with the shaved head took charge, warning us that we needed to “take the proper permissions to be here.” He introduced himself as “a local political leader.” We later found out that he was [Jagadesh Np](#)—one of the owners of Spencer Apparel, a dyeing company that makes clothes for an Indian department store chain, Westside.

When I called Spencer Apparel, a man who identified himself as Rajesh Np, Jagadesh’s brother, got on the line. At first, he yelled, questioning angrily why we had been on the grounds of the government industrial park without special permission. After talking for a few minutes, he changed tack, suddenly inviting us back. “I can give you a detailed explanation about everything and show you everything so that you can write a very good article,” he said. And he promised, “In Tirupur, most of us do eco-friendly dyeing. Everything is nonhazardous.”

But as Vidiyal Sekar, a former Tamil Nadu state legislative assembly member representing Tirupur, points out, “Eighty percent of dyers do not properly discharge their waste.” Sekar did not speak directly to the practices at Spencer Apparel. But he added that much of the blame should be placed on TNPCB officials, anyway: “All the pollution department officers do is take a lot of money from these small factories and allow them to operate freely.” The TNPCB, Sekar says, is “100 percent corrupt.”

Lack of accountability means that it’s nearly impossible to figure out which companies were legally operating dyeing plants and which were not. In June 2013, I spoke numerous times on the phone with then-TNPCB Member Secretary S. Balaji, who was steadfastly evasive. In July 2013, H. Malleshappa replaced Balaji. Malleshappa also did not answer any phone messages from *Newsweek*. Late in 2013, a group of environmentalists [launched](#) a public interest lawsuit to remove Malleshappa from office, claiming that he was unqualified. Malleshappa eventually left the position soon after an incident in which almost [1,000 illegal bottled water](#) plants were found in his district. Much of the water was unsafe for human consumption. Despite the scandal, Malleshappa remains in a position of power: He is now head of the state’s [Department of the Environment](#). His replacement at the TNPCB, K. Karthikeyan, didn’t last long either. He was [forced out](#) when a local crusading journalist revealed that Karthikeyan had been under investigation for corruption when he was appointed.



Records show that Raagam sold clothing to major companies like Ecko, Desigual and New Era over the past decade. NEWSWEEK

.....

operations. But the court found that only the TNPCB's head office in Chennai could grant them permission to reopen—and that they still hadn't achieved the zero-liquid discharge required for that consent. In October 2011, [the court dismissed Raagam's case](#).

Borja Castaneda, Desigual's marketing director, says the company has been working with Raagam since 2012. "They have the temporary license to run the dyeing unit," Castaneda wrote in an email to *Newsweek*. "This license has been annually renewed (including the one for 2015) as they are still pending to receive the final one." However, Desigual was unable to provide documentation of the licensing. It was also unable to send over documentation of the audits it claims to undertake regularly. "Unfortunately, these are confidential," said Castaneda.

Raagam Exports was also unwilling to provide proof of its license to operate; its website has a "Compliance" section, but does not include any TNPCB licensing. And the TNPCB website provides nothing that can help to ascertain whether Raagam is currently licensed. Meanwhile, the company continues to send clothes to international brands—Desigual, for example, received its most recent shipment—almost 260 pounds of multihued viscose dresses—from Raagam in July 2015.

The Gap Gap

P.N. Shamuhasundar runs [Mastro Colours](#), a small hosiery dyer on Tirupur's outskirts. The state government gave him and about 20 other dyers a \$4 million, no-interest loan to overhaul and modernize their shared effluent treatment plant. Mastro is now certified as having "zero liquid discharge," but the extra cost of treating and evaporating that liquid waste (instead of just dumping it into the river) means it can't compete with polluting dyers.

Prithviraj believes American consumers are complicit here. “We feel that selling a T-shirt for \$10 is a sin,” he says. “Is it fair Wal-Mart makes \$8 off a T-shirt and gives nothing to the labor, nothing to the environment?”

Shipping records provided by Datamyne, which tracks import-export transactions in the Americas, show that between 2007 and 2011, Wal-Mart’s orders increased from Tirupur clothing companies who dyed garments in defiance of the court-ordered shutdown. Take Balu Exports, for example. On its website, the company describes itself as a “vertical set-up under one roof.” Two of its divisions, Balu Process and Balu Exports Dyeing, are members of the Dyers Association of Tirupur. And since 2007, the association has operated in contempt of [India’s Supreme Court order](#) to reach zero discharge.



During the 2000's Wal-mart's orders from Balu Exports increased, despite the fact that the company was operating an illegal dyeing factory. NEWSWEEK

Repeated inquiries to Wal-Mart over the years about its reliance on toxic dyeing companies have been unanswered. In 2015, after receiving detailed shipping records and documentation highlighting the illegal operating status of Balu and other companies from which Wal-Mart sources, Juan Andres Larenas Diaz, director of communications for international corporate affairs, sent a written statement to *Newsweek*: “Our expectation and a contractual requirement of doing business with us is that our suppliers and their subcontractors are in compliance with the law. Our relationship with garment suppliers in Tirupur has always been based on their ability to meet Wal-Mart’s supplier standards and code of conduct.” But Diaz would not address

specific allegations.

Prithviraj says he’s been similarly frustrated in attempts to engage Wal-Mart. Talking to Wal-Mart is like “banging your head against a wall,” he says. Instead, he suggested, we should try asking some “big brands”—like Gap, J.C. Penney, Tommy Hilfiger—about their record in Tirupur.

Gap Inc. has long been on the radar of environmental activists. Every year, Greenpeace’s garment monitoring unit—called the [Detox Catwalk](#)—places major clothing companies in three categories: winners, greenwashers and losers. Gap Inc. is one of the most well-known

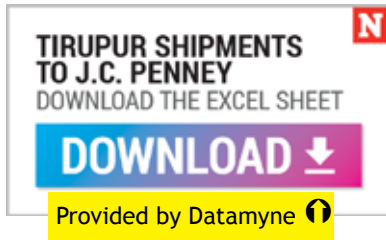
“losers,” based on the company’s refusal to disclose hazardous chemicals and unwillingness to commit to stop using them.

Over the past 15 years, Gap Inc. has increasingly outsourced its manufacturing. The company says it has a field team of 40 sustainability experts around the world who make both announced and unannounced visits to nearly all of the factories where its clothing is made. However, it also has come to rely on inspection from third-party firms in order to ensure its indirect suppliers—such as mills and dyers—are adhering to the company’s vendor code of conduct.

In its 2011-2012 Social and Environmental Responsibility Report (the most recent publicly available), Gap Inc. admits that it does not have direct control over its supply chain, and things appear to be getting worse. In 2005, 10 to 24.99 percent of its factories in South Asia had violations in their Vendor Code of Conduct- mandated environmental management systems; by 2012, that rose to over 50 percent.

“If over 50 percent of their suppliers are not in compliance, then environmental issues are not a factor in the Gap's supplier selection process,” says Heather White, a supply-chain expert and fellow at Harvard University’s Edmond J. Safra Center for Ethics . White adds that in many cases, factories end up paying auditors for an inspection report, and in those cases, “the quality of the findings suffers.” That’s because auditors are more likely to keep their jobs if the factories pass inspections. Bribery is common, White says—though she was not able to speak directly to activities within Gap’s supply chain.

The issue, ultimately, is that the compliance measures taken by retailers like Gap, Desigual and the dozens of other firms sourcing garments in Tirupur don’t account for the complexity of modern clothing-supply chains. Fabric is frequently taken from a mill, dyed at a second facility (owned by the same parent company) and then sewn into finished garments at a third factory (ditto). A corporate auditor, examining the factory and the final product, would find it difficult to determine where the cloth has been dyed. Even visiting a dyeing facility isn’t enough; it’s easy for a given dyeing facility to subcontract some portion of its dyeing orders to smaller, unauthorized units. And it’s even unlikely that an inspector is present when effluent is treated—or released directly into the Noyyal, or dumped in a local field in the middle of the night. Auditing and even TNPCB approval, says Prithviraj, provide little more than a veneer of plausible deniability. “It’s a very sophisticated system of lying,” he says.



Over the last decade, J.C. Penney has taken shipments from many Tirupur-based exporters, including Eastman Exports, which also runs an illegal dyeing operation. NEWSWEEK

A representative for J.C. Penney, for example, told *Newsweek* that “to the best of our knowledge it does not appear that J.C. Penney has any dyeing business in that area,” despite records showing that the company has been taking shipment for years from numerous vertically integrated manufacturers in the Tirupur area, including Eastman Exports. Eastman was [operating in contempt of India’s Supreme Court](#) 2007 demand that it reach zero effluent discharge during the time it sold garments to J.C. Penney. But since the American giant was able to buy from its “finishing” arms, it could feasibly deny knowledge of the illegal dyeing operations involved. “We confirmed with Eastman Exports that no dyeing services were performed for J.C. Penney's private brand merchandise in those factories,” its representative wrote in an email. Eastman did not respond to requests for comment.

According to Gap Inc., the situation in South India has improved dramatically in recent years. Spokeswoman Laura Wilkinson told *Newsweek* that all the company’s third-party auditors are paid for by corporate, and as of June 30, 2015, approximately 90 percent of the company’s approved facilities in South Asia have an environmental management system. “We recognize there is a still long way to go,” says Wilkinson, “and it will require sustained, and collective, effort to have the most lasting impact.”

Many of the other companies that rely on factories in South and East Asia offer similar promises. “Since we are operating in a water-intense industry, we have worked actively to reduce negative water impacts in different parts of the value chain for more than 10 years,” says Ulrika Isaksson, an H&M spokeswoman. “Our goal is to become the fashion industry’s leading water steward.” (H&M is one of [Greenpeace's “winners”](#); it also publishes a [supplier list](#), which includes both primary manufacturers and secondary suppliers like dyers.) Others, including Uniqlo and Tommy Hilfiger, did not respond to multiple requests for comment.

Gap, for its part, has made a [commitment](#) to achieve zero liquid discharge in all its supplier factories by 2020. But even if it makes good on the promise, for many farmers in and around Tirupur, it’s likely to be too late.

Rotten Coconuts

When I returned to Tirupur in January 2015, the Orathupalayam Dam was still filled with green, foamy water. The few locals who have remained in the area struggle to survive.

Karuppaiah Subramanyam has lived and farmed near the dam for many years. From his house, I could see some scrub grass and a smattering of coconut trees, but when I looked a little more closely, the damage became clear: The coconuts—his only crop—were undersized, and many came off the tree already rotten. Subramanyam's 7-acre farm, which was in his family for several generations, remains the same size it's always been, but it has now become essentially worthless. When Tirupur's clothing industry began producing more clothes and even more toxic runoff, he lost about half his crop, because his primary water source became unusable. "We can only do rain-fed agriculture now," he explains. Before 1995, he could grow eggplant, green chilies, tomatoes, rice, turmeric and tobacco. Now he has to buy all that on the market, with the meager funds he gets from his remaining, undernourished coconuts.

Asked whether he ever received compensation for his losses, he simply shakes his head. There were some court cases, but only the largest landholders with the best legal representation were compensated. Smaller farmers, like Subramanyam, got nothing. Prithviraj led 4,000 of these excluded farmers in an appeal to the Madras High Court, which ultimately decided they should all be remunerated by the dyers association for land that was made barren by the release of toxic textile runoff. Still, that's only a fraction of the nearly 30,000 farmers Prithviraj estimates lost their livelihood.

Meanwhile, illegal dyeing units continue to surface regularly. "Some of the new dyeing factories are coming up in other river basins and even in the coastal areas," says Prithviraj. He mentions Cuddalore, an ancient seaport town about 200 miles east, where chemical pollution in some areas has already raised the risk that residents will contract cancer in their lifetimes at least 2,000 times that of the average person.

Even if all the polluting ceased immediately, the damage is already done; it might be impossible to clean and regenerate the Noyyal River and the soil along its basin, says Prithviraj. "We'd have to turn back the clock 20 years."

Additional reporting by Aletta Andre and Anil Varghese.

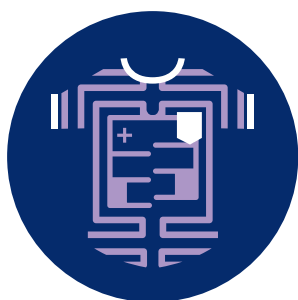


The Global Language of Business

Transforming the Retail Supply Chain

Apparel, Fashion and Footwear





“Implementing EPC-enabled RFID technology has been one of the most significant technological steps Macy’s has taken toward improving our supply chain performance, and ultimately our customer service, in the last 20 years. It is one of the keys to our omni-channel success, and because we’ve already seen solid results, we plan to expand its use, as our business growth and consumer loyalty depend on it.”

– Peter Longo, President of Logistics & Operations, Macy’s

Collaborating in the dynamic retail industry

In today’s omni-channel retail world, consumers are in control. They have embraced social media, online search and mobile apps—giving them instant access to product information to make buying decisions.

Consumers are driving a retail environment where fast fashion translates to high-speed product turnover and a vast number of stock-keeping units that must be managed. On the supply side, retail production is complex and truly global in scope where brands and manufacturers alike source materials and labour from a worldwide network of suppliers.

This dynamic retail industry calls for increased collaboration across the supply chain for improved speed-to-market capabilities and efficiencies. Partners in the apparel, fashion and footwear (AFF) sector are looking to inventory management and procurement processes to help drive these improvements.

Inventory Accuracy with EPC/RFID

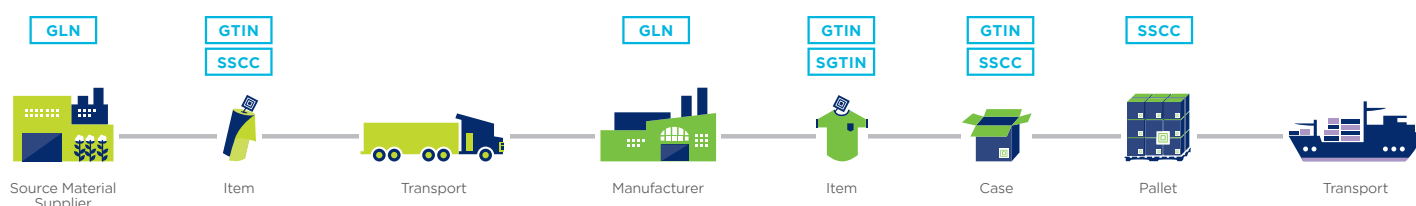
Industry leaders are starting to “tag at the source” by applying GS1 EPC-enabled RFID tags on items at the point of manufacture. Using standards-based product identifiers—Serialised Global Trade Item Numbers (SGTINs) encoded into EPC tags, manufacturers can provide true visibility of merchandise as it travels to distribution centres and stores.

Brand owners utilise EPCs to easily verify the accuracy and completeness of shipments received—each identified by a GS1 Serial Shipping Container Code (SSCC)—and can track shipping processes to reduce counterfeits from entering the supply chain.

Retail distributors can monitor the progress of incoming and outgoing shipments via EPCIS, a GS1 standard used to share information about the physical location and status of products. This increased visibility enhances their ability to trace products back to their sources for verification of sustainability, and track their paths to stores that ultimately receive them.

EPCs are used by distributors to confirm that the right products are included in shipments and that their inventory databases are automatically updated. As shipments arrive at final destinations, stores read EPCs to confirm they have received the right products.

EPC/RFID technology helps retail stores track inventory levels, which in turn reduces out-of-stocks and speeds inventory counts. EPC is also used for point of sale transactions and can help prevent inventory loss through electronic article surveillance. And with EPC-enabled RFID innovations, retailers are creating exciting shopping experiences such as “smart” fitting rooms where shoppers, for example, can scan a product to find which colours and sizes are in stock or receive helpful fashion advice.



The GLN identifies any type or level of location such as a building or department. • The GTIN uniquely identifies a trade item such as a product or service.

Procurement Precision with GS1 Standards

Another major opportunity for AFF industry partners is using GS1 standards in upstream procurement processes.

GS1 identification standards such as Global Trade Item Numbers (GTINs) and Global Location Numbers (GLNs) in combination with GS1 electronic communication standards can be used throughout order, fulfilment and invoice processes to accurately communicate information about merchandise and supply chain locations.

Using EPC/RFID, stores benefit from greater inventory accuracy—and issue purchase orders for only the merchandise they need. Product GTINs can be listed on the orders and electronically communicated via EDI for faster processing.

Distribution centres fulfil the orders by picking and reading inventoried merchandise to ensure the right products are included in shipments to the right stores. Advance Ship Notices or Despatch Advices are electronically communicated to stores before the arrival of merchandise. Upon arrival, stores can easily compare the actual products received against what products were ordered. Invoices can also include the GTINs of products received for accurate and quick electronic payments.

The underpinning of these efficient procurement processes is having accurate master product data—an asset that is becoming increasingly important, especially in e-commerce.

By adopting GS1 standards, AFF partners can cut through the complexity of retail's global supply chain for better ways to collaborate and conduct business. And with the rise of omni-channel retail and the resulting proliferation of business partners, the adoption of global standards is more urgent than ever before.

“We have decided to follow GS1 standards when using EPC/RFID for identification of shipments and single items and sharing this data with our partners through EPCIS. By using GS1 standards along the entire supply chain, we can get rid of its huge complexity and improve speed-to-market intervals.”

– Joachim Wilkens, Unit Leader of Supply Chain Development, C&A Europe

Learn how GS1 standards can help you significantly improve your business processes.

Visit www.gs1.org/retail.

Contact your GS1 Member Organisation; see www.gs1.org/contact.

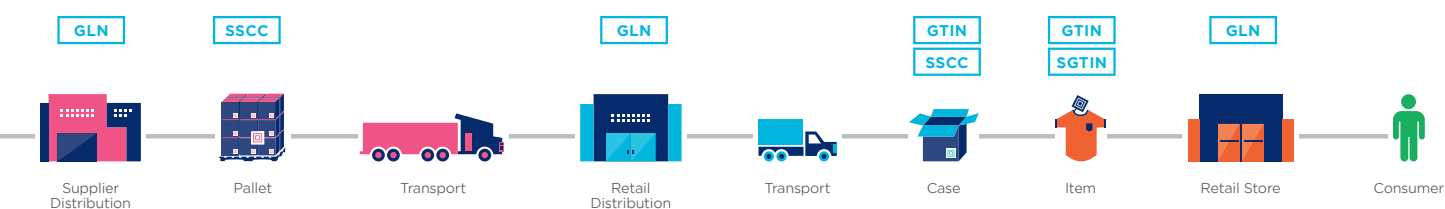
Levi Strauss Takes Control

Levi Strauss & Co. employs about 5,000 people and manages 50 production centres in more than 110 countries. In 2005, the company decided it needed more reliable and precise control of its inventory.

Pilots were initiated to implement EPC/RFID item-level tagging and technologies in its Mexico operations, including stores, a distribution centre and manufacturing plant. Based on exceptional pilot results, Levi Strauss decided to extend GS1 EPC/RFID standards to improve business processes in its remaining stores.

Results from the EPC/RFID implementation are impressive, and include:

- Reduced in-store inventory from 4-month to 2-month supplies
- Improved inventory accuracy to 99 percent when comparing on-shelf inventory levels with those in the company's system
- Increased sales by 11 percent
- Reduced lost sales by 40 percent due to reduction in out-of-stock merchandise



The SGTIN is a serialised GTIN that uniquely identifies an individual trade item. • The SSCC identifies a logistic unit such as a case, pallet or parcel.

“GS1 standards allow us to drive availability and efficiencies across our omni-channel supply chain, improving the experience for customers and profitability for partners.”

- Terry Murphy, Director of National Distribution Centres, John Lewis

About GS1

GS1 is a neutral, not-for-profit, global organisation that develops and maintains the most widely used supply chain standards system in the world. GS1 standards improve the efficiency, safety, and visibility of supply chains across multiple sectors. With local Member Organisations in over 110 countries, GS1 engages with communities of trading partners, industry organisations, governments, and technology providers to understand and respond to their business needs through the adoption and implementation of global standards. GS1 is driven by over a million user companies, which execute more than six billion transactions daily in 150 countries using GS1 standards. More information at www.gs1.org.

GS1 AISBL

Blue Tower, Avenue Louise 326, bte 10

BE 1050 Brussels, Belgium

T +32 2 788 78 00

E contactus@gs1.org

www.gs1.org



FASHION TRANSPARENCY INDEX

APRIL 2016

02	WHY TRANSPARENCY IS THE BEGINNING OF A FASHION REVOLUTION
05	RESEARCH METHODOLOGY
07	THE FASHION TRANSPARENCY INDEX RESULTS
13	WHAT DO THE RESULTS SHOW?
15	POSITIVE EXAMPLES
16	CONCLUSION
17	GET INVOLVED
18	REFERENCE & APPENDIX
19	ABOUT THIS REPORT

The content of this publication can in no way be taken to reflect the views of any of the funders of Fashion Revolution.

© Fashion Revolution CIC 2016.
All rights reserved. This document is not to be copied or adapted without permission from Fashion Revolution CIC.

WHY TRANSPARENCY IS THE BEGINNING OF A FASHION REVOLUTION

*Three years ago on
24th April, 1,134
people were killed
in the Rana Plaza
garment factory collapse
in Bangladesh.*

The factories operating in that building made clothes for over a dozen well-known international clothing brands. It took weeks for some companies to determine whether they had contracts with those factories despite their clothing labels being found in the rubble.

Fashion Revolution and Ethical Consumer feel passionately that tragedies like Rana Plaza must never happen again. Today, both people and the environment suffer as a result of the way fashion is made, sourced and purchased. It's time for a Fashion Revolution, and we believe that the beginning of this process is transparency.



COMPLEXITY OF SUPPLY CHAINS

Fashion supply chains are typically long and very complex. Some brands may work with thousands of factories at any given time – and that is just the facilities that cut, sew and assemble our garments, but there are also further facilities down the chain that dye, weave and finish materials and farms that grow fibres too. During the manufacturing process our clothes are touched by a great many pairs of hands before they reach the rails or shelves of the shop floor.

Many companies do not really know where their clothes are being made. The vast majority of today's fashion brands do not own their manufacturing facilities, making it difficult to monitor or control working conditions throughout the supply chain. A brand might place an order with one supplier, who carves up the order and subcontracts the work to other factories. This happens regularly across the industry and presents a great challenge for brands themselves as well as the people working in the supply chain who become invisible in this process.

THE IMPORTANCE OF TRANSPARENCY

Lack of transparency costs lives. It is impossible for companies to make sure human rights are respected and that environmental practices are sound without knowing where their products are made, who is making them and under what conditions. If you can't see it, you don't know it's going on and you can't fix it.

Transparency means companies know who makes their products – from who stitched them right through to who dyed the fabric and who farmed the cotton. When companies are working in a transparent way, this also implies openness, communication and accountability across the supply chain and with the public too.

At the moment the public do not have enough information about where and how their clothes are made. Shoppers have the right to know that their money is not supporting exploitation, human rights abuses and environmental destruction. There is no way to hold companies and governments to account if we can't see what is truly happening behind the scenes. This is why transparency is essential.

Being transparent creates the opportunity for collaborative action between companies, governments, NGOs, unions and the public to work towards building a fairer, cleaner and safer fashion industry.

We need more transparency from the fashion industry. Transparency involves openness, communication and accountability.

THE FASHION TRANSPARENCY INDEX

Together Ethical Consumer and Fashion Revolution wanted to find out what companies are doing towards improving social and environmental standards and how much of that information they share with the public.

As a first step, Fashion Revolution and Ethical Consumer have partnered up to publish a Fashion Transparency Index which ranks companies according to the level of transparency in their supply chain.

The first edition of the Fashion Transparency Index includes 40 of the biggest global fashion brands, which we have selected based on annual turnover. We relied on publicly available financial information to choose this selection of brands and their inclusion was not voluntary. We aimed to choose brands from a variety of sectors – high street, luxury, sportswear, accessories, footwear and denim.

For consumers, the Fashion Transparency Index aims to give you some insight into just how little we know about the things we buy and wear. We hope it encourages you to want to find out more about the story of your clothes.

For brands and retailers, we hope the Fashion Transparency Index inspires you to publish more about your policies, practices, products and the people making your clothes – answering the question **#whomademyclothes**.

There is no doubt that the goal of transparent fashion supply chains is challenging. But we are beginning to see that some companies are beginning to make a real effort while others have a long way to go. With this Index, we hope to track the fashion industry's progress towards greater transparency, ensuring that together we are pushing for more information and better practices.

We want more brands and retailers to be able to answer the question **#whomademyclothes?**



RESEARCH METHODOLOGY

The Fashion Transparency Index uses a broad brushstroke approach.

The research has been designed to give you an illustrative look at how much brands know about their supply chains, what kind of policies they have in place and importantly, how much information they share with the public about their practices and products. As such, the Index does not offer an in-depth analysis of the content of a company's policies or performance in any given area.

It uses a ratings methodology, which benchmarks companies against current and basic best practice in supply chain transparency in five key areas:

POLICY & COMMITMENT

What are the standards and goals the company sets itself for the protection of workers and the environment across its supply chain? What information do they make public about these policies and commitments?

TRACKING & TRACEABILITY

How well does the company know its supply chain, and what information do they share publicly about who and where products are made?

AUDITS & REMEDIATION

How does the company go about checking its supply chain for compliance with its policies, international standards and local laws? How does the company deal with its suppliers that fail to meet these obligations? How much information do they make public about these activities?

ENGAGEMENT & COLLABORATION

To what extent does the company work with multi-stakeholder initiatives, NGOs, unions and civil society to tackle social and environmental issues in its supply chain? And are these activities communicated publicly?

GOVERNANCE

What checks and balances does the company have in place and who is responsible within its own organisation for ensuring initiatives that address labour standards are implemented? And what information regarding governance is publicly available?

RESEARCH METHODOLOGY

continued

All 40 companies included in the index were invited to fill out a questionnaire, which helped us to better understand their policies, activities and communications.

In total we received 10 replies, and the other 30 were scored based upon information available on their website and in their annual reports.

For the companies that did not reply, it is impossible for our researchers to know anything beyond what they are communicating publicly online. Therefore these companies may have received lower scores while companies who did fill out the questionnaire had the opportunity to tell us more and thus potentially score higher. Any company wishing to have their score updated may do so if new information is made available for our research team to investigate.

This means that overall the companies publishing the most information about their supply chain practices online or via other public communication channels will likely have received the higher scores.

Broadly, under each key area marks were allocated on a sliding scale summarised below:

● LOW RATING

Little to no evidence that the company has more than a Code of Conduct in place. The company is making little effort towards being transparent about their supply chain practices.

● LOW-MIDDLE / ● HIGH-MIDDLE RATING

The company is making some notable efforts on social and environmental issues, but could be doing much more.

● TOP RATING

The company is making significant efforts in the given areas, and has made some or most of this information publicly available.

The top scores **do not** mean that the company has a fully transparent supply chain or is acting beyond its policy commitments. Whilst these companies should be congratulated for providing more information about their practices and products than most, there is a long way to go before any of the companies included in this Index will be able to fully answer **#whomademyclothes**.

THE RESULTS

0-25%

LOW RATING

Chanel
 Hermes
 Claire's Accessories
 Forever 21
 Fendi
 LVMH
 Monsoon Accessorize
 Prada
 Michael Kors
 Aeropostale
 Under Armour

26-50%

LOW-MIDDLE

Ralph Lauren
 Polo Ralph Lauren
 URBN
 New Look
 Gucci
 Victoria's Secret
 Hugo Boss
 J Crew
 ASOS
 Burberry
 Coach
 Lululemon
 Next
 Abercrombie & Fitch
 Arcadia Group
 Topshop
 Mango

51-75%

HIGH-MIDDLE RATING

American Eagle
 Gildan Activewear
 Uniqlo
 Converse
 Nike
 PVH
 Gap
 Primark
 Adidas

76-100%

TOP RATING

H&M
 Inditex
 Levi Strauss & Co

THE RESULTS

continued

	POLICY & COMMITMENTS %	TRACKING & TRACEABILITY %	SOCIAL & ENVIRONMENTAL AUDITS & REMEDIATION %	ENGAGEMENT & COLLABORATION %	GOVERNANCE %	QUESTIONNAIRE %	TOTAL SCORE %
Chanel	0	0	29	0	0	✗	10
Hermes	43	0	21	0	14	✗	17
Claire's Accessories	29	0	29	0	14	✗	17
Forever 21	14	0	43	0	14	✗	19
Fendi	14	0	43	0	14	✗	19
LVMH <small>*Berluti, Céline, Dior, Donna Karan, EDUN, Emilio Pucci, Fendi, Givenchy, Kenzo, Marc Jacobs, Moynat, Loewe, Loro Piano, Louis Vuitton, Nicholas Kirkwood, Thomas Pink, R.M. Williams</small>	14	0	43	0	14	✗	19
Monsoon Accessorize	29	11	29	10	14	✗	20
Prada <small>*Prada, Miu Miu, Church's, Car Shoe, Marchesi 1824</small>	43	22	7	20	29	✓	21
Michael Kors	29	0	50	0	0	✗	21
Aeropostale	29	11	43	0	14	✗	24
Under Armour	29	0	43	10	29	✗	25
Ralph Lauren <small>*Including Club Monaco</small>	57	0	57	0	29	✗	33
Polo Ralph Lauren	57	0	57	0	29	✗	33

THE RESULTS

continued

	POLICY & COMMITMENTS %	TRACKING & TRACEABILITY %	SOCIAL & ENVIRONMENTAL AUDITS & REMEDIATION %	ENGAGEMENT & COLLABORATION %	GOVERNANCE %	QUESTIONNAIRE %	TOTAL SCORE %
URBN <small>*Urban Outfitters, Anthropologie, Free People, BHLDN, Terrain, Vetri Family</small>	29	33	43	0	43	✓	33
New Look	57	33	21	50	43	✗	37
Gucci <small>*part of the Kering group</small>	64	33	29	10	43	✗	38
Victoria's Secret	64	0	64	10	43	✗	40
Hugo Boss	50	11	71	0	43	✗	42
J Crew	57	22	57	10	43	✗	42
ASOS	64	28	43	20	57	✗	43
Burberry	64	6	50	20	71	✗	43
Coach	57	11	64	0	57	✗	43
Lululemon	71	39	50	20	29	✗	44
Next	71	28	43	50	43	✗	45
Abercrombie & Fitch	71	11	64	20	43	✗	45
Arcadia Group <small>*Topshop, Burton Menswear, Dorothy Perkins, Evans, Miss Selfridge, Outfit, Topman, Wallis</small>	64	50	50	10	57	✗	49
Topshop	64	50	50	10	57	✗	49

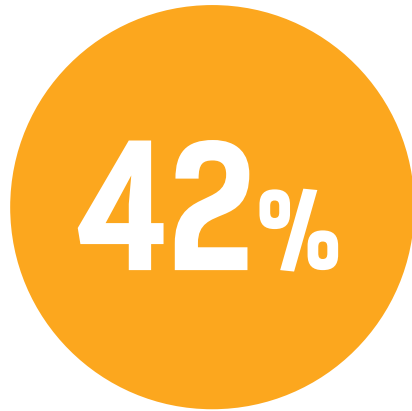
THE RESULTS

continued

	POLICY & COMMITMENTS %	TRACKING & TRACEABILITY %	SOCIAL & ENVIRONMENTAL AUDITS & REMEDIATION %	ENGAGEMENT & COLLABORATION %	GOVERNANCE %	QUESTIONNAIRE %	TOTAL SCORE %
Mango	57	33	64	40	43	✗	50
American Eagle	57	28	79	30	43	✗	52
Gildan Activewear	57	22	71	40	71	✓	55
Uniqlo	79	11	71	40	71	✗	56
Converse	79	39	57	20	86	✗	57
Nike <small>*Nike, Nike+, Jordan, Converse, Hurley</small>	79	39	57	20	86	✗	57
PVH <small>*Calvin Klein, Tommy Hilfiger, Van Heusen, IZOD, ARROW, Speedo, Warner's, Olga</small>	64	44	79	40	43	✓	58
Gap <small>*Gap, Banana Republic, Old Navy, Athleta, Intermix</small>	100	44	71	50	57	✓	65
Primark	86	56	64	60	71	✓	67
Adidas	79	72	71	80	57	✓	69
H&M <small>*H&M, COS, Weekday, Monki, Cheap Monday, & Other Stories</small>	79	83	71	80	71	✓	76
Inditex <small>*Zara, Bershka, Pull&Bear, Massimo Dutti, Stradivarius, Oysho, Zara Home, Uterqüe</small>	79	61	93	80	100	✓	76
Levi Strauss & Co <small>*Levi's, Dockers, Signature, Denizen</small>	86	61	86	60	86	✓	77

THE RESULTS

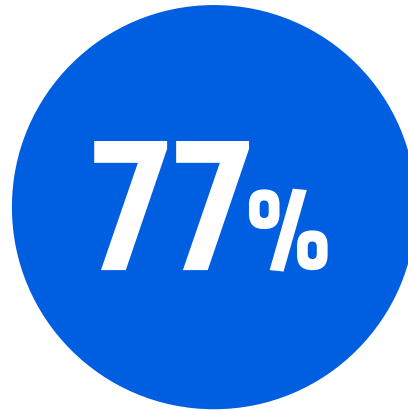
continued



AVERAGE SCORE



*for the 40 brands
we surveyed*



TOP SCORE



Levi's Strauss & Co



BOTTOM SCORE



Chanel

A ROUGH GUIDE TO THE SCORING

0-25%

These companies have little to no information about their supply chain practices available to the public. Many of these companies seem to do little more than have a Code of Conduct in place – whilst this might have been best practice in the 1990s, Corporate Responsibility has moved on a great deal in the last twenty years. These companies appear to be those at the beginning of the road towards best practice and transparency.

POSITIVE STEPS TAKEN:

Minimal

ROOM FOR IMPROVEMENT:

All areas

26-50%

These companies seem to be making some efforts to manage and improve their supply chains but make little supply chain information publicly available. These companies still have a long way to go towards supply chain transparency.

POSITIVE STEPS TAKEN:

Policies and commitments in place and some steps taken in other areas

ROOM FOR IMPROVEMENT:

Auditing & reporting; tracking & traceability; engagement & collaboration & governance; and more transparent communications.

51-75%

These companies seem to be doing a bit more than the others when it comes to having policies and commitments in place and auditing and reporting activities. Despite making some good efforts to monitor standards, these companies seem to be lacking in many areas and offer some public supply chain transparency but not enough.

POSITIVE STEPS TAKEN:

Policy & commitment; auditing & reporting

ROOM FOR IMPROVEMENT:

Tracking & traceability; engagement & collaboration; governance; and more transparent communications.

76-100%

Only three companies have scored in this range. Levi Strauss & Co scored highest with 77. They are doing more than most other brands to communicate publicly about their supply chain practices. They seem to have many robust systems in place for tracking, tracing, monitoring and improving labour and environmental practices across the supply chain. The other two companies to score a top rating are H&M and Inditex both come in just one percentage point behind Levi's at 76%. However all the companies in this section still have a long way to go towards being fully transparent.

POSITIVE STEPS TAKEN:

All areas

ROOM FOR IMPROVEMENT:

More stakeholder engagement; better tracing of products down to sources of raw material; and even more transparent communications with the public.

WHAT DO THE RESULTS SHOW?

Strongest areas:

POLICY & COMMITMENT

In this area, the majority of the companies score well on having policies on environmental and labour standards in place and communicating them publicly. But there is a noticeable absence of long-term thinking in their sustainability strategies.

Only three of the companies (Gap, Primark, Levi Strauss & Co.) appear to be looking to the future with clear long-range (2020 or beyond) aims, which include defined end-goals and quantified targets along the way – as well as an explicit commitment to transparency.

H&M, Inditex and Nike (which includes Converse) are the only other companies to publish quantifiable targets towards improving standards and performance across the supply chain over time. However, they do not appear to communicate any specific targets on transparency.

Additionally, only a few companies show evidence of policies that target the engagement of suppliers further down the supply chain, eg. engaging directly with fabric mills.

AUDITING & REMEDIATION

Most companies provide information on audit procedures and schedules publicly, along with some limited disclosure of audit results. Levi Strauss & Co appears to publish the most information about their monitoring practices and corrective action plans.

Roughly 28% of companies do not communicate about taking any special measures to monitor the more difficult issues in the supply chain (eg. improving conditions for homeworkers, eliminating forced labour, or eradicating Sumangali practices, a form of child labour), nor disclose in detail how they work with factories that show non-compliances in order to ensure they improve working conditions.

Many companies surveyed have legal obligations to monitor and disclose supply chain issues via the California Transparency in Supply Chains Act of 2010, which means a company must disclose on its website its initiatives to eradicate slavery and human trafficking from its direct supply chain for the goods offered for sale. A company must disclose to what extent it: (1) engages in verification of product supply chains to evaluate and address risks of human trafficking and slavery; (2) conducts audits of suppliers; (3) requires direct suppliers to certify that materials incorporated into the product comply with the laws regarding slavery and human trafficking of the countries in which they are doing business;

(4) maintains accountability standards and procedures for employees or contractors that fail to meet company standards regarding slavery and human trafficking; and (5) provides employees and management training on slavery and human trafficking. A similar law has just come into effect in the UK, the Modern Slavery Act 2015 and applies to companies with an annual turnover of £36 million or more. However, most luxury brands surveyed offer little to no public information about how they monitor working conditions, with the exception of Burberry, Hugo Boss and Michael Kors.

GOVERNANCE

60% of companies surveyed appear to have a system in place to monitor compliance with labour standards, and to continually improve standards, with responsibility at the executive board level.

WHAT DO THE RESULTS SHOW?

Weakest areas:

TRACKING & TRACEABILITY

Just over half the companies (60%) surveyed seem to be making some efforts in this area, such as holding internal databases of their cut-make-trim (CMT) suppliers – the ‘first tier’ of the supply chain.

Only five brands (Adidas, H&M, Levi Strauss & Co, Nike – which includes Converse) reflect best practice in holding a publicly available list of all or the vast majority of their CMT suppliers. 24 companies state that they track their suppliers and/or their locations, but do not publish this information publicly. 12 companies appear not to track the first tier of their supply chain, or at least this information is not publicly available.

Only two companies (Adidas and H&M) publish details of their second-tier suppliers (fabric and yarn mills or subcontractors). However, the majority of the 40 companies surveyed appear to have little (30% of companies surveyed) or nothing (53%) in place to demonstrate that they monitor where raw materials and other resources (such as zips and other component parts) come from.

The ‘second tier’ of the supply chain (and third, fourth, etc.) seems to remain largely unknown territory for most companies surveyed.

ENGAGEMENT & COLLABORATION

Only 11 of the companies in the Index show evidence of working with trade unions, civil society or NGOs on the ground in supplier countries to improve working conditions. Trade unions in particular are vital in providing garment workers with the means to demand better working conditions and pay from their employers.

The Engagement & Collaboration part of the Index also looks at membership of Multi-Stakeholder Initiatives (MSIs). MSIs bring together lots of different stakeholders in order to find common solutions to problems, such as the Ethical Trading Initiative, Sustainable Apparel Coalition, Textile Exchange and others.

Our list of MSIs includes the Bangladesh Accord, an initiative set up in the wake of the Rana Plaza factory collapse, working to ensure improved health and safety standards in Bangladesh’s garment factories. Given that Bangladesh is the world’s second largest garment exporter, many of the companies included in the Index are likely to be sourcing from the country. In this Index we considered participation in the Accord important.

However, not every company in this Index will be sourcing from Bangladesh but because most do not publish their factory lists we do not know which companies are sourcing from this country.

A majority of companies (26) are involved with at least a few of the eight MSIs that we looked for engagement with. But no company is a member of all eight initiatives. 14 companies surveyed, mostly luxury brands, do not appear to engage with any of them at all, showing a lack of industry collaboration on social and environmental issues.

GOVERNANCE

19 of the companies surveyed (40%) do not appear to have a system in place to monitor compliance with labour standards and to continually improve standards, both at Board level (eg. an executive corporate responsibility committee) and at departmental level (eg. a Social Responsibility team). Human rights and environmental protection should be the responsibility of company executives as well as at department level. In addition 15 companies (38%) show no evidence of incorporating labour standards into buying practices.

We are also surprised by the large number of companies (30%) that do not appear to have whistleblowing or confidential complaint mechanisms in place for workers in their supply chain, or at least none that they mention publicly. This means that workers may have little chance to speak up about poor conditions or abuse, or may not be able to do so without fear of repercussion.

POSITIVE EXAMPLES

'SUPPLIER CLUSTERS'

Inditex has 10 [supplier clusters](#) in the geographic areas in which it has a larger and stronger presence: Spain, Portugal, Morocco and Turkey (these four countries comprise about 60% of the company's supply chain); India, South East Asia, Bangladesh, China, Brazil and Argentina. These clusters covered 91% of Inditex's production in 2014 and "are regularly consistently under review". Through these clusters, Inditex works with trade unions, NGOs and civil society on labour rights.

PUBLISHING FACTORY LISTS

[Adidas publishes a list of subcontractors](#) (eg. specialist printing, mould production, or embroidery services) as well as a CMT list on its website. [H&M has mapped 99% of its production volume](#), publicly publishes 95% of its first tier CMT list and 35% of its fabric and yarn suppliers. In this area both Adidas and H&M demonstrated the highest levels of transparency of all 40 companies in this Index.

WORKING WITH NGOS AND TRADE UNIONS

Gildan works with the Maquila Solidarity Network – a labour and women's rights advocacy organisation that promotes solidarity with grassroots groups in Mexico, Central America and Asia, and works to improve conditions in maquiladora factories and export processing zones. The company says: "Through dialogue with MSN, we have applied their input in the development of a remediation plan following the closure of our El Progreso plant in Honduras. Since then, [Gildan](#) has been working collaboratively with the MSN regarding labour practices and freedom of association at its various manufacturing locations. We continue to remain in dialogue with MSN regarding our corporate social responsibility practices."

INTEGRATED REPORTING

Kering Group (the company that owns Gucci) has developed a tool to measure and calculate the financial value of its environmental impacts throughout its supply chain – known as [Environmental Profit & Loss](#). Its 2013 report revealed that 93% of the Group's environmental impact falls within its supply chain. In 2015 Kering made the EP&L methodology open-source.

PUBLISHING LIFECYCLE ANALYSIS RESEARCH

[Levi Strauss & Co](#) has set itself the goal to increase the percentage of its own products made with Water<Less™ techniques to 80% by 2020 – a technique to reduce water used in wet processing of jeans and other clothes. Levi's has also published a lifecycle analysis of a pair of jeans, which sets out the impacts at different stages of manufacture. The company has made its research publicly available online so that other companies can make use of it.

GOING BEYOND 1ST TIER

[Gap](#) partnered with 20 strategic mills in China, India, Pakistan and Taiwan to conduct environmental assessments using the Sustainable Apparel Coalition's Higg Index and has since expanded the programme to include 20 more strategic mills in 2015.

CONCLUSION

Big global brands have a lot of work to do to show their commitment to transparency.

Some companies are taking steps in the right direction, Levi Strauss & Co, H&M and Inditex offer the most information about their policies, strategies and performance on social and environmental issues throughout the supply chain. However, there is a lot they don't tell the public too, especially when you look past the first-tier.

Publishing supplier lists for the first-tier is possible; some brands have done it but not nearly enough. Inditex says it doesn't publish its factory list for commercial reasons, but we have to move beyond that line of thinking. If H&M, Adidas, Nike and Levi's can do it and remain profitable then other companies can too. This is an important first step to ensure that brands are accountable to their stakeholders and to their customers – those asking **#whomademyclothes** now number in the millions.

Overall, every brand should be doing more to communicate with the public about their strategies and performance on social and environmental issues throughout the supply chain. But the luxury brands are the biggest laggards; most publish nothing more than a Code of Conduct.

Going forward Fashion Revolution will encourage brands to publish more details about the suppliers they work with, and we will celebrate them when they do.

We would also like to see brands put in place sustainability strategies, covering both social and environmental improvements, with clearer long-term goals that include timelines, quantifiable targets and an explicit commitment towards greater transparency. This shows that brands are serious about doing more for the people who make their products.

Going forward Fashion Revolution will encourage brands to publish more details about the suppliers they work with, and we will celebrate them when they do.

GET INVOLVED

This Index is a living document and is open to comments and contributions from researchers, NGOs and unions.

We also invite the 40 companies scored in this Index to provide further information in order to update their score. Where companies did not respond to our questionnaire, we were only able to assign marks based on the information we could find on the company's website or publicly available elsewhere. As such, the scoring is likely to evolve over time when new information becomes available.

We further invite brands and retailers over £36 million annual turnover to volunteer to be included in future editions of the Fashion Transparency Index. **Next year we aim to include 100 brands and retailers in this Index.**

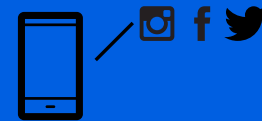
If you are a consumer and would like to see another brand on the Fashion Transparency Index, let them know on social media or write to them. Don't forget to use the hashtag **#whomademyclothes**.



SHOW YOUR LABEL



ASK THE BRAND
#WHOMADEMYCLOTHES?



REFERENCE & APPENDIX

To see the full methodology and research behind the scores, please visit:

www.ethicalconsumer.org/ethicalcampaigns/fashionrevolution

10 brand questionnaires completed in March 2016.

Business Insider (6 July 2015). **The top 10 clothing companies in America.** Retrieved: uk.businessinsider.com/the-10-biggest-apparel-companies-in-the-us-2015-7?r=US&IR=T

California Transparency in Supply Chains Act of 2010. Retrieved: www.state.gov/documents/organization/164934.pdf

Chain Store Guide. **The Top 100 Apparel Specialty Stores Ranked by Industry Sales.** Retrieved: www.chainstoreguide.com/static_content/pdf/Apparel_Top_100.pdf

Millward Brown (2015). **BrandZ Top 100 Most Valuable Global Brands.** Retrieved: www.millwardbrown.com/BrandZ/2015/Global/2015_BrandZ_Top100_Chart.pdf

Modern Slavery Act 2015, United Kingdom. Retrieved: www.legislation.gov.uk/ukpga/2015/30/contents/enacted

Reuters (9 July 2013). **Bangladesh garment sales soar despite deadly incidents.** Retrieved: www.reuters.com/article/us-bangladesh-economy-exports-idUSBRE96806020130709

Statista (2015). **Brand value of the leading 10 apparel brands worldwide in 2015.** Retrieved: www.statista.com/statistics/267931/brand-value-of-the-leading-10-apparel-brands-worldwide/

The Bangladesh Accord on Fire and Building Safety. Retrieved: bangladeshaccord.org

The Richest (17 December 2013). **10 Most Powerful Luxury Brands in the World.** Retrieved: www.therichest.com/expensive-lifestyle/fashion/10-most-powerful-luxury-fashion-brands-in-the-world/?view=all

The UK Fashion Spot (1 July 2014). **The 5 Most Valuable Fast Fashion Brands.** Retrieved: www.theukfashionspot.co.uk/runway-news/422009-the-most-valuable-fast-fashion-brands/

ABOUT THIS REPORT

*This research was
designed by Ethical
Consumer in partnership
with Fashion Revolution.*

The research was carried out by Bryony Moore, Ethical Consumer research associate, with additional input from Tim Hunt (Ethical Consumer) and Sarah Ditty (Fashion Revolution).

This report was co-written by Bryony Moore at Ethical Consumer and Sarah Ditty; and designed by Heather Knight. Thanks for further input from Carry Somers at Fashion Revolution and the entire Fashion Revolution Global Coordination Team.



FASHION REVOLUTION is a global movement that wants to radically change the way fashion is made, sourced and consumed. We believe in an industry that values people, the environment, creativity and profit in equal measure. We have teams in 89 countries that want to see fashion become a force for good.

www.fashionrevolution.org

 [@Fash_Rev](https://twitter.com/@Fash_Rev)

 [Fash_rev](https://www.instagram.com/Fash_rev)

 facebook.com/fashionrevolution.org



ETHICAL CONSUMER is a research co-operative with a mission to make business more sustainable through consumer action. For over 25 years we have been the heart of the ethical consumer movement, helping consumers to shop ethically, campaigners to challenge corporate power and businesses to improve their supply chain.

www.ethicalconsumer.org

 [@ec_magazine](https://twitter.com/@ec_magazine)

 facebook.com/ethicalconsumermagazine

Compliance is Not Enough:

Best Practices in Responding to The California Transparency in Supply Chains Act



Compliance is Not Enough:

Best Practices in Responding to The California Transparency in Supply Chains Act

The California Transparency in Supply Chains Act has focused company attention on the presence of human trafficking and modern-day slavery in supply chains. Yet standard social compliance responses will not be adequate to reduce company risks – or worker vulnerability – to these egregious problems.

In this White Paper, Verité outlines the content of the Act, the sources of trafficking and forced-labor risk, and what is necessary in order to address these problems adequately in supply chain production.

What Is the California Transparency in Supply Chains Act & What Does It Require?

In October 2010, Senate Bill 657 – the California Transparency in Supply Chains Act – was signed into law. This Act goes into effect on January 1st, 2012 and applies to all retailers and manufacturers with annual global revenues of more than \$100 million that do business in California. The Act requires these businesses to disclose information about their efforts to eradicate slavery and human trafficking from their direct supply chains where they make tangible goods for sale.

To review the full text of the Act, [click here](#).

The stated purpose of the Act is “to educate consumers on how to purchase goods produced by companies that responsibly manage their supply chains, and, thereby, to improve the lives of victims of slavery and human trafficking.”¹ Some groups have suggested that the Act will provide companies in California with the opportunity to demonstrate leadership in the fight against human trafficking, while empowering consumers to reward companies that proactively engage on these issues.

The Act requires businesses to publicly post information on their websites describing the extent to which they engage in the following:

- **Verification:** Verify product supply chains to evaluate and address risks of human trafficking and slavery;
- **Auditing:** Perform supplier audits to evaluate compliance with company standards;
- **Certification:** Require certification by direct suppliers that materials incorporated into company products comply with the laws regarding slavery and human trafficking of the country or countries in which they are doing business;
- **Internal Accountability:** Maintain internal accountability standards and procedures for employees or contractors that fail to meet company standards on slavery and trafficking; and
- **Training:** Train relevant company employees and management on human trafficking and slavery, particularly concerning the mitigation of risk within supply chains.

Businesses are required to post their disclosure with a “conspicuous and easily understood” link on their website homepage leading to the required information. In the event that they do not have a website, companies are obliged to provide consumers with written disclosure within 30 days of receiving a written request.

The penalty for non-compliance with the Act is injunctive relief by the California Attorney General. This means companies will not face a monetary penalty for failure to disclose, but that they will receive an order from the Attorney General to take specific action.

Standard social compliance responses will not be adequate to reduce company risks – or worker vulnerability – to these egregious problems.

One estimate by the California Franchise Tax Board indicates that approximately 3,200 companies will be affected by the Act. This includes manufacturers and retailers with their headquarters in the state, as well as national and international companies that do business there. Suppliers to these companies that operate outside California, though not legally bound by the Act, may be affected by it as their business partners take action to meet their new obligations under the law. The Act is poised to become a de facto standard for performance by all companies, and indeed a version of the Act has been introduced at the Federal Level.²

How Should Companies Respond? Going Beyond Compliance to a Systems-Based Approach

To meet the letter of the California Transparency in Supply Chains Act, companies need only publicly disclose the extent of their own policies and practices to eradicate slavery and human trafficking. But this is clearly not enough. Companies should instead commit to finding trafficking and forced labor where they exist in the supply chain, and resolving these abuses where they are found.

To fully understand and prevent trafficking and slavery in the making of products requires a greater level of effort and commitment. Detecting, preventing, and taking corrective action against slavery, trafficking, and forced labor in a supply chain presents substantial challenges to 'business-as-usual' efforts to implement social compliance. In Verité's experience, it is impossible to identify the hidden and insidious abuses of human trafficking and forced labor unless a company examines all aspects of workers' employment, from the moment of recruitment to on-site employment, across the entire supply chain. If companies are serious about eradicating trafficking and forced labor, they must also look beyond their first-tier suppliers to ensure that businesses deep in their supply chains are mirroring their own commitments.

To fully understand and prevent trafficking and slavery in the making of products requires a greater level of effort and commitment.

Some companies already have well-established compliance or responsible sourcing programs to monitor and promote improvements in their supply chains that include many of the functions mentioned in the California Act. These programs, however, often fail to fully address the particular abuses targeted by the Act, namely, the trafficking of persons and forced labor. These programs also frequently neglect the common risks of exploitation posed to migrant workers linked to unscrupulous labor brokers at the recruitment and hiring phases in the supply chain.

Here are the steps that companies need to take to ensure that they do not engage in forced labor and human trafficking in their internal and supply chain operations:

Detection, Assessment & Auditing

Discovering slavery and trafficking requires a bright light to be shone in all the places where a company manufactures or sources goods and raw materials. The causes of these abuses are complex, and their manifestations are often hidden. Assessing situations of trafficking and slavery requires companies to consider the many intertwined factors that leave workers vulnerable. In supplier audits, many of these factors can only be learned from workers themselves, so it is essential that companies engage workers through confidential interviews, conducted off-site by qualified interviewers. Only this approach to assessment can guarantee that workers are not working against their will.

Detection of forced labor, trafficking, and slavery in a company's supply chain also requires an understanding that workers are vulnerable from the moment they are first recruited for a job. This is when workers can take their first steps along the route into forced labor or slavery. Though the California law only requires that companies disclose how they deal with their 'direct suppliers,' Verité believes that companies must recognize the likelihood that egregious practices also exist among the sub-contracted business partners that provide first-tier suppliers with hired labor or materials (including the materials that go into stores and other facilities). Risks of trafficking and forced labor for companies exist at top-tier supplier factories and through the actions of often-overlooked labor brokers involved in the recruitment and hiring process. These risks are also frequently found in second and lower tiers of the supply chain, including at the commodities and raw-materials levels.

Integrating Solutions into the Business Management System

A worker-focused assessment or audit of a farm or factory is only one component of an effective system for preventing forced labor and human trafficking throughout supply chains. Broadly credible policies and procedures that screen for these risks and measure the performance of suppliers and labor brokers must be integrated into companies' entire legal compliance and corporate social responsibility (CSR) programs and cover the entirety of the supply chain – not only the top tier. This is a clear challenge for companies that source from several thousand farms or factories worldwide.

Broadly credible assessments must be integrated into companies' entire legal compliance and corporate social responsibility programs and cover the entirety of the supply chain – not only the top tier.

Truly sustainable prevention and eradication of slavery and human trafficking requires that companies make prevention efforts part of the way they do business, integrating the avoidance of exploitation with mechanisms for hiring workers, sourcing suppliers, and measuring business success.

Corporate-Level Engagement

At the corporate level, companies should explicitly prohibit these abuses in their codes of conduct, policy statements, and supplier selection and management practices; and ensure that exploitation linked to trafficking and abuses by labor brokers is addressed. Companies need to identify the populations of workers that are most vulnerable, and the places of greatest risk within their supply chains, in order to target assessment, prevention, and remediation efforts. Understanding risk is critical to targeting often-limited resources to the right part of a large and multi-tiered supply chain. Companies then need to raise awareness and build capacity within their own ranks and within those of their suppliers to take action against these abuses.

Workplace-Level Engagement

At the farm or factory level, employers and workers also need to be trained and educated on labor risks, so that they can play a critical role in rooting out abusive conditions on the front lines. Systems must be in place to prevent these issues from occurring in the first place – for example, by integrating appropriate controls at each stage in the recruitment, hiring, placement, employment, and on-site management of workers. Factory or farm personnel with the appropriate training may be able to spot these problems by asking the right questions and knowing what to look for. Involving first-tier suppliers as active and vital partners can help companies look deeper into sub-contracting and the suppliers of raw materials, parts, and labor. Orienting and training workers is also a critical step to ensuring that vulnerability to abuse is identified and corrected, and exploitative conditions are remediated. Some companies that operate in difficult legal environments in which the vulnerability of workers is exacerbated by legislative or public policy conditions (for example the legally allowed withholding of passports) may also wish to engage in policy advocacy to promote regulatory circumstances that minimize rather than contribute to risk for companies and workers.

CASE STUDY: Forced Labor at a Malaysia-Based Factory

Verité recently conducted a social assessment for one of the pioneers in the social responsibility sector – a global company that sells fast-moving consumer goods in stores around the world. For the assessment, Verité visited a Malaysia-based workshop where flooring and countertops were manufactured for the company's Asian stores. At the workshop, employment and living conditions were shocking: Nepalese, Burmese and Bangladeshi migrants were paid only once every three months and reported being regularly harassed verbally. They lived in shipping containers that had been converted into living areas and which suffered from water leaks, poor sanitation, and excessively high temperatures. Workers' movements were restricted by gates that were locked at night and the presence of a guard dog in the courtyard. These conditions can be classified as forced labor.

If managers throughout the global company's supply chain had been trained on the risks of nontraditional procurement and incentivized to find suppliers with ethical work practices, this scenario would not have unfolded. Verité knew of suppliers of similar materials in the same geographic area that had much better working conditions.

What Are the Risks to Companies of Slavery & Human Trafficking?

The risks of slavery and human trafficking in supply chain production are significant. Anywhere from 12 to 27 million people are victims of slavery and other forms of forced labor worldwide, and more than 2.4 million of these victims have been trafficked.³

Trafficking and slavery are widespread: One hundred and sixty one countries are either a source, transit, or destination country for trafficking in persons.⁴ Slavery and other types of forced labor are found in both the informal and formal economies, and in a wide range of sectors and services. In the United States, for example, ten thousand or more people are being forced to work at any given time. Victims of forced labor in the US are found in sectors including domestic service, the sex industry, food processing, hospitality, factory production, and agriculture.⁵

The challenges to combating slavery and trafficking in the manufacturing of goods are complex and multifaceted. These abuses are sometimes obvious but in many cases hidden and difficult to identify. Verité's research has shown that slavery can be present in diverse circumstances and at many levels of supply chain production.⁶ It is most common at the base of the supply chain, in the harvesting or extraction of raw materials (for example, food, fiber, or oil crops; and fish, timber, gold, and other minerals) and during different stages of the manufacturing of finished products.⁷ Companies concerned with the California Act may also run a particular risk of employing forced laborers in the construction of their facilities or stores overseas; and in the maintenance, servicing or management of those facilities, in cases where those functions are outsourced to a third-party supplier.

Because slavery and trafficking can manifest themselves in many different settings and situations, it is important for businesses to understand the different risk factors that can contribute to these severe forms of abuse. It is also important to recognize that social compliance efforts to-date have focused primarily on the workplace itself, and not on the paths that workers take to arrive at their jobs. Verité's *in-depth research* and results from thousands of worker interviews at workplaces around the world reveal the many ways in which exploitation in recruitment and hiring can pave the way for workers to become trapped in their jobs.

During Recruitment & Hiring

Workers are highly vulnerable when they are recruited into their jobs. Migrant workers especially can be deceived by the promise of high wages and good working conditions. Common causes of vulnerability include:

- **Deception** – Workers are told by a recruiter (the employer or an employer's agent) that they will receive high wages and be provided with good living conditions, but find the opposite upon arrival at the worksite.
- **Debt** – Workers may incur debt from paying fees to employers and recruiters for their jobs. Illegally high fees and loans taken at excessive interest rates can trap workers in a kind of bonded labor. Workers arrive at the worksite to find that wages are much lower than promised. After interest and debt repayments, these workers are often left with minimal or no income.
- **Contract Substitution** – Workers may be asked to sign an employment contract in a language they do not understand, or are asked to sign a new, replacement contract (with lower wages and benefits) when they start work.

CASE STUDY: Benny

Benny graduated from a four-year computer school in the Philippines and was unable to find work. He borrowed money to pay a recruiter for a legal job in an IT factory in Taiwan. When Benny got to Taiwan, he discovered that his recruitment debt had been increased by 150 percent, and his salary was half of what he was expecting.

Benny worked six to seven days a week, 12 hours a day with mandatory overtime for two years. When his contract was up, he returned home having barely dug himself out of the recruitment debt. With no savings and his family reeling from a storm that flooded their home, Benny plans to return to Taiwan to try again. This time, he says he hopes to go with an "honest" recruiter.

Migrant workers especially can be deceived by the promise of high wages and good working conditions.

- **Trafficking** – Workers are transported to a remote worksite away from family, friends, and any support structure, in debt and without any means to escape. Migrant workers, often from among the rural poor, may travel overseas or long distances within their own country to obtain a job.

Verité has encountered these vulnerabilities in many sectors, including electronics, garments, construction, and agriculture. Taken together or on their own, they place workers in extreme situations of risk that can result in forced labor, coercion and human trafficking.

During Employment

Slavery and forced labor can be perpetuated at the job site when employers keep workers trapped using different mechanisms of control:

Slavery and forced labor can be perpetuated at the job site when employers keep workers trapped.

- **Withholding Personal Identity Documents** – Especially for foreign migrant workers, the employer may hold workers' identity documents, making it impossible for them to cross borders or avoid being detained by authorities. In one case, Verité found that a labor broker in a Southeast Asian country told workers that if they questioned their employment conditions, he would rip up their passports and report them to the police as illegal immigrants.
- **Financial Control** – An employer may control workers by withholding wages until the end of a contract or until a crop is planted to prevent them from terminating employment. They may also attempt to control workers through debt (e.g., by providing advances or loans with high interest rates) or by controlling their bank accounts and withholding ATM cards.
- **Physical or Sexual Abuse** – Workers may be subjected to physical or sexual abuse or inhumane disciplinary practices if they question their working conditions or disobey the rules. In situations of trafficking, vulnerability to sexual abuse can be high. For example, Verité found in its research that, under the Sumangali scheme in southern India, young girls are promised a lump sum of cash as dowry money after a multi-year contract, but instead work long hours in deplorable conditions and can face threats of sexual exploitation.
- **No Freedom of Movement & Housing** – Workers are locked in their housing or in the workplace under strict supervision. Verité has found cases where workers are either not allowed to leave the farm or factory compound at all, or may only do so every few months with an escort. In another case, Verité found workers housed in shipping containers in a locked factory compound patrolled by pit bulls.

CASE STUDY: Fernando

Fernando from Guatemala wanted to earn more money to send his children to school. He contracted with a labor broker to obtain an H-2B visa for temporary work on tree plantations in the southeastern United States. He borrowed the money for the \$2,000 recruitment fee.

Upon arrival in the US, Fernando and 11 other migrants were piled into a van and driven through the night to New England, to do plant nursery work. This work was not covered by his visa. Fernando was suddenly illegal.

Fernando's passport was confiscated, and he was required to sign a contract that he could not read. He was placed in overcrowded housing an hour from the jobsite. He worked 12 to 15 hour days six days a week, for around US \$1.20 an hour after deductions, under constant verbal threat.

Fernando eventually escaped and filed a lawsuit with other victims. The parent company of the nursery settled out of court, and the victims were awarded a small sum, but not enough to pay off their recruitment debts. Fernando is still living and working in the United States to pay of his debt. He misses his family.

Each of these coercive mechanisms must be considered when attempting to detect slavery, forced labor, and trafficking in a company supply chain. Assessment measures should be adopted or refined to ensure that auditors have the full means to detect cases of abuse, and companies

should establish systematic preventive measures to guard against them. Comprehensive corrective action strategies and systems improvement plans should also be established in the event that a case of forced labor or human trafficking is discovered in the company or supply chain.

How Verité Provides Solutions

Verité's services and resources can help companies to fully understand the nature and sources of slavery and human trafficking in supply chains and how to overcome the obstacles to building sustainable systems solutions that benefit companies and workers alike. These services provide the skills, knowledge, and training needed not only to meet and exceed the obligations companies face under the California Act but to identify and root out the deceptive and coercive practices that lead workers into situations of trafficking and forced labor in supply chains.

Embedding the capacity, knowledge, and systems-based approach across the entire supply chain helps companies effectively and comprehensively meet their new obligations under Bill 657.

Assessment and Consultation

Verité provides both online resources and consultation to help companies identify and address forced labor risks.

Resources

- Verité's **Help Wanted initiative** helps companies ensure their products are made under fair, safe, and legal conditions.
- Verité's **Fair Hiring Framework for Responsible Business** and **Fair Hiring Toolkit** provide strategies and comprehensive tools and guidance to support responsible recruitment in global supply chains. These open-source materials are invaluable in providing a roadmap and practical tools to help companies take action against the abuses facing migrant workers.
- Standards of verification for ethical brokerage, forthcoming from Verité and the Manpower Group, provide a call to action and guidance for companies and other stakeholders on this critical issue.
- Our on-line **Commodity Atlas** provides considerations to determine the risks of forced labor in production.

These tools provide companies with the means to analyze their product supply chains and to evaluate their exposure to the risk of human trafficking and slavery.

Consulting

Our consulting assists companies in identifying risks of trafficking, slavery, and forced labor in their supply chains. Verité's consulting helps brands and suppliers identify existing gaps in their business processes that do not effectively screen for risks of trafficking and forced labor, and supports development of strong, internal accountability mechanisms to combat these abuses, imbedded in suppliers' existing business management systems and processes.

Auditing Services

Verité's worker-focused audits are uniquely positioned to detect indicators of trafficking, slavery, and forced labor. Standard social audits are generally unable to uncover forced labor, particularly when it involves foreign migrant workers and abuses perpetrated by labor brokers. Verité has conducted social audits that have identified how much workers were overcharged by brokers, and facilitated repayment to those workers.

Capability Building and Training

Verité training programs have provided suppliers, managers, and regional/corporate CSR staff on farms and in factories with knowledge and skills to eliminate forced labor abuses. Verité's Migrant Labor Workshops help companies manage the risks inherent in using brokered labor, helping participants to understand the manifestations and root causes of human trafficking and debt-bondage. Classroom-based learning of this kind will soon have an online component, with the development of a comprehensive eLearning platform, which addresses the California Act and risks of forced labor and human trafficking.

Embedding the capacity, knowledge, and systems-based approach across the entire supply chain helps companies illuminate the risks of forced labor, establish effective preventive measures, respond systematically to cases of human trafficking, and effectively and comprehensively meet their new obligations under Bill 657.

Who is Verité?

Verité is an international not-for-profit consulting, training, and research NGO that has been a leader in supply chain social responsibility and sustainability since 1995. Verité is a member of the Alliance to End Slavery and Trafficking, and has presented its solutions to forced labor at the Clinton Global Initiative. For its work, Verité was winner of the Skoll Award for Social Entrepreneurship in 2007 and the Schwab Social Entrepreneur of the Year Award for 2010.

For more information, please contact Verité at +1.413.253.9227 or Dr. Shawn MacDonald, Senior Advisor at smacdonald@verite.org.

References:

- ¹ See: http://info.sen.ca.gov/pub/09-10/bill/sen/sb_0651-0700/sb_657_bill_20100930_chaptered.html
- ² See: <http://maloney.house.gov/press-release/maloney-introduces-bipartisan-bill-fight-human-trafficking>
- ³ International Labor Organization. *A global alliance against forced labor*. Geneva. 2005.
- ⁴ United Nations Office on Drugs and Crime. *Trafficking in Persons, Global Patterns*. Vienna, 2006.
- ⁵ Free the Slaves and Human Rights Center, University of California, Berkeley. *Hidden Slaves: Forced Labor in the United States*. September 2004.
- ⁶ Verité. *Help Wanted: Hiring, Human Trafficking & Modern-Day Slavery in the Global Economy*. June 2010.
- ⁷ See: <http://www.dol.gov/ilab/programs/ocft/PDF/2011TVPRA.pdf>.

SOURCEMAP ([/#HOME-SECTION](#)) SUPPLY CHAIN VISUALIZATION ([/#RESTAURANT-SECTION](#))
TRACEABILITY ([/#SUBSUPPLY-CHAIN-MAPPING-SECTION](#)) SUSTAINABILITY ([/#TRANSPARENCY-1-SECTION](#))
RISK & COMPLIANCE ([/#NEW-PAGE-1-SECTION](#)) PRICING ([/#DEMO-1-SECTION](#)) MORE

JANUARY 24, 2017 ([/BLOG/2017/1/24/SOURCEMAP-SELECTED-FOR-NEXT-GENERATION-HIGG-INDEX](#))

SOURCEMAP SELECTED FOR NEXT GENERATION HIGG INDEX



At Sourcemap, we believe that consumers have the right to know the social and environmental impact of products. That's why we're thrilled to have been selected as the new Higg Index platform, the leading suite of tools for measuring social and environmental sustainability across the apparel, footwear and textile industries. The Higg Index was developed by the Sustainable Apparel Coalition, a multi-stakeholder organization whose members include Walmart, Nike, H&M, the Gap - in all

190+ brands, retailers, manufacturers, NGOs and academic institutions around the world.

The platform represents a huge step forward in supply chain transparency, enabling companies to measure sustainability across their complete supply chains, with the goal to share the results with consumers in the near future.

"The Sustainable Apparel Coalition is thrilled to work with Sourcemap on the next generation Higg Index online platform. Sourcemap will bring all of the diverse sets of sustainability information that SAC collects together and help usher in a new era of improvement and transparency for the apparel, footwear and textile industries." - Jason Kibbey, CEO, Sustainable Apparel Coalition

Sourcemap's work with the Sustainable Apparel Coalition is rooted in a shared vision of collaboration across supply chains to bring about system-wide change. We are proud to work with the SAC and its members to steward the future of sustainable fashion.



Collin Thompson [Follow](#)

Blockchain Product Designer & Growth Marketer

Oct 2, 2016 · 6 min read



Blockchain ABC and 123

How does the Blockchain Work (for Dummies) explained simply

How does the Blockchain Work? Well here is a simple explanation that cuts through the hype.

Blockchain is a hot topic around the world these days, yet for many, the technology remains an elusive concept. Yet it shouldn't, the concept is simple once you get your head around the architecture and theory of basic crypto economics. When you do have your "a Ha" moment, the world will never seem the same to you again.

This blockchain basics guide is designed to deliver a clear, non-technical introduction to one of the most transformational & misunderstood technologies of our time. If you want to know what blockchain technology is, how it works, and it's potential impacts, without all the technical lingo, then this post is for you.

A short History of Transacting Money

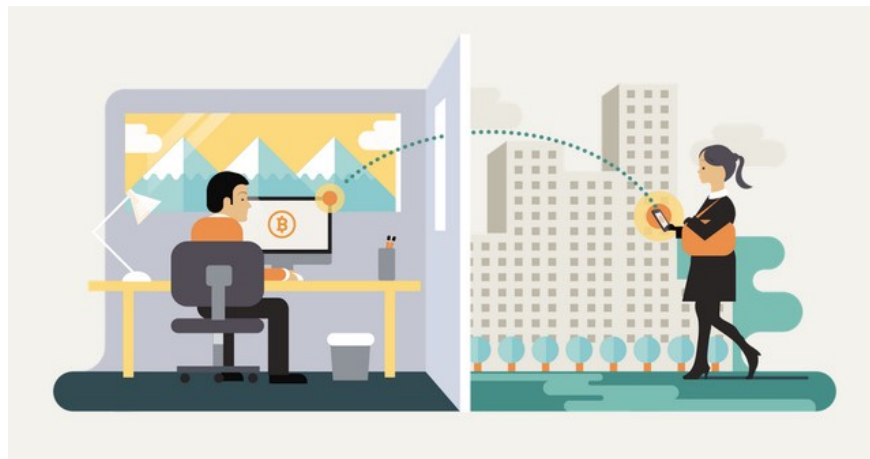
Historically, when it comes to transacting money or anything of value, people and businesses have relied heavily on intermediaries like banks and governments to ensure trust and certainty.^[1] Middlemen perform a range of important tasks that help build trust into the transactional process like authentication & record keeping.^[2]

The need for intermediaries is especially acute when making a digital transaction. Because digital assets like money, stocks & intellectual property, are essentially files, they are incredibly easy to reproduce. This creates what's known as the double spending problem (the act of spending the same unit of value more than once) which until now has prevented the peer to peer transfer of digital assets.^[3]

But what if there was a way of conducting digital transactions without a third party intermediary? Well, a new technology exists today that makes this possible. But before we dive into the mechanics of this revolutionary technology, it's important to provide a little context.

Blockchain Vs Bitcoin—What's the connection?

Bitcoin first appeared in a 2008 white paper authored by a person, or persons using the pseudonym Satoshi Nakamoto. The white paper detailed an innovative peer to peer electronic cash system called Bitcoin that enabled online payments to be transferred directly, without an intermediary.^[4]



how the blockchain transfers value

Via (techliberation.com)

While the proposed bitcoin payment system was exciting and innovative, it was the mechanics of how it worked that was truly revolutionary. Shortly after the white paper's release, it became evident that the main technical innovation was not the digital currency itself but the technology that lay behind it, known today as blockchain.

Although commonly associated with Bitcoin, blockchain technology has many other applications. Bitcoin is merely the first and most well-known uses. In fact, Bitcoin is only one of about seven hundred applications that use the blockchain operating system today.^[5]

“[Blockchain] is to Bitcoin, what the internet is to email. A big electronic system, on top of which you can build applications. Currency is just one.” ^[6]—Sally Davies, FT Technology Reporter

One example of the evolution and broad application of blockchain, beyond digital currency, is the development of the [Ethereum public blockchain](#), which is providing a way to execute peer to peer contracts.^[7]

What's under the blockchain hood?

Blockchain is a type of distributed ledger or decentralized database that keeps records of digital transactions. Rather than having a central administrator like a traditional database, (think banks, governments & accountants), a [distributed ledger](#) has a network of replicated databases, synchronized via the internet and visible to anyone within the network.^[8] Blockchain networks can be [private with restricted](#) membership similar to an intranet, or public, like the Internet, accessible to any person in the world.^[9] ^[10]

When a digital transaction is carried out, it is grouped together in a cryptographically protected block with other transactions that have occurred in the last 10 minutes and sent out to the entire network. Miners (members in the network with high levels of computing power) then compete to validate the transactions by solving complex coded problems.^[11] The first miner to solve the problems and

validate the block receives a reward. (In the Bitcoin Blockchain network, for example, a miner would receive Bitcoins).

The validated block of transactions is then timestamped and added to a chain in a linear, chronological order. New blocks of validated transactions are linked to older blocks, making a chain of blocks that show every transaction made in the history of that blockchain.^[12] The entire chain is continually updated so that every ledger in the network is the same, giving each member the ability to prove who owns what at any given time.

“A blockchain is a magic computer that anyone can upload programs to and leave the programs to self-execute, where the current and all previous states of every program are always publicly visible, and which carries a very strong cryptoeconomically secured guarantee that programs running on the chain will continue to execute in exactly the way that the blockchain protocol specifies.”—Vitalik Buterin

Blockchain’s decentralized, open & cryptographic nature allow people to trust each other and transact peer to peer, making the need for intermediaries obsolete. This also brings unprecedented security benefits. Hacking attacks that commonly impact large centralized intermediaries like banks would be virtually impossible to pull off on the blockchain. For example—if someone wanted to hack into a particular block in a blockchain, a hacker would not only need to hack into that specific block, but all of the preceding blocks going back the entire history of that blockchain. And they would need to do it on every ledger in the network, which could be millions, simultaneously.

^[13]

Will the blockchain transform the Internet & the global economy?

Make no mistake about it. Blockchain is a highly disruptive technology that promises to change the world as we know it. The technology is not only shifting the way we use the Internet, but it is also revolutionizing the global economy.^[14]

By enabling the digitization of assets, blockchain is driving a fundamental shift from the Internet of information, where we can

instantly view, exchange and communicate information to the Internet of value, where we can instantly exchange assets.^[15] A new global economy of immediate value transfer is on its way, where big intermediaries no longer play a major role. An economy where trust is established not by central intermediaries but through consensus and complex computer code.^[16]

“The technology likely to have the greatest impact on the next few decades has arrived. And it’s not social media. It’s not big data. It’s not robotics. It’s not even AI. You’ll be surprised to learn that it’s the underlying technology of digital currencies like Bitcoin. It’s called the blockchain.”—Don Tapscott

Blockchain has applications that go way beyond obvious things like digital currencies and money transfers. From electronic voting, smart contracts & digitally recorded property assets to patient health records management and proof of ownership for digital content.

Blockchain will profoundly disrupt hundreds of industries that rely on intermediaries, including banking, finance, academia, real estate, insurance, legal, health care and the public sector—amongst many others.^[17] This will result in job losses and the complete transformation of entire industries.^[18] But overall, the elimination of intermediaries brings mostly positive benefits. Banks & governments for example, often impede the free flow of business because of the time it takes to process transactions and regulatory requirements. The blockchain will enable an increased amount of people and businesses to trade much more frequently and efficiently, significantly boosting local and international trade. Blockchain technology would also eliminate expensive intermediary fees that have become a burden on individuals and businesses, especially in the remittances space.

Perhaps most profoundly, blockchain promises to democratize & expand the global financial system. Giving people who have limited exposure to the global economy, better access to financial and payment systems and stronger protection against corruption and exploitation.^[19]

“Every human being on the planet with a phone, will have equal access. Expanding the total addressable market by 4X”—Brock Pierce

The potential impacts of blockchain technology on society and the global economy are hugely significant. With an ever growing list of real-world uses, blockchain technology promises to have a massive impact. This is just the beginning.

Many of the most exciting applications and platforms haven't even been invented yet!

— -

I'm always interested in meeting blockchain startups, and technologists who are creating innovative products, so please feel free to contact me on [linkedin](#) , or by email at collin@intrepid.ventures

Collin Thompson is the Co-founder, and Managing Director of Intrepid Ventures, a blockchain startup and innovation studio that invests, builds, and accelerates Blockchain and FinTech companies solving the world's most difficult problems. Collin focuses on early stage investments, innovation and business design for corporations, governments and entrepreneurs working with blockchain technology.



Blockchain's Smart Contracts: Driving the Next Wave of Innovation Across Manufacturing Value Chains

Smart contracts with embedded business rules promise not only to reduce transaction costs but to create more agile value chains that enable closer cooperation and enhanced trust across the extended manufacturing ecosystem.

Executive Summary

Blockchain – the cryptocurrency technology with the potential to eliminate financial services intermediaries – may also have the power to fundamentally change the manufacturing industry as we know it. By allowing supply chain partners to create trusted relationships without the need for banks or, perhaps, even traditional purchasing processes, manufacturers, suppliers, customers and machines can find each other and do business much more quickly and inexpensively.

Even more importantly, they will be able to form more agile supply chains through “smart contracts” that automatically find, negotiate with and close deals with partners the world over. This will help all participants across the value chain to speed new products to market that meet ever-changing business needs, and will enable more trusted and fruitful relationships.

But leveraging blockchain will require carefully balancing risks versus benefits, integrating new technologies and processes with legacy systems and evaluating the maturity of the required technologies, standards and providers. It will also

require overcoming resistance from both government and established intermediaries such as banks.

This white paper explains blockchain, what it means for the manufacturing industry and how to begin using it to drive quantum leaps in efficiency, agility and innovation.

Blockchain Explained

Blockchain is a software mechanism, now primarily known in the form of bitcoin in the financial services world, that provides a distributed system of trusted assets and transactions without the need for a central trust authority.

For manufacturers and their suppliers or logistic partners, an individual transaction in a block might contain bills of lading for raw materials or finished goods, proof of the origin, quality or operations performed on a part or instructions for the place and time of a delivery. In each case, the information could be stored, trusted, shared and changed by the partners without going to the cost, expense and delay of negotiating formal contracts or paperwork such as letters of credit from a bank or a bond for a transportation provider.



Unlike in a traditional supply chain, where these documents and contracts are maintained by each partner's purchasing, accounting or legal department, in a blockchain these elements are stored on many decentralized nodes. Their privacy and integrity is maintained by "miner-accountants" rather than by a counterparty or a third party such as a bank (see Figure 1).

Blockchain enables the creation of smart contracts, with terms and conditions both sides can specify and that assure trust in the enforceability of the contract and the identity of the counterparty.

Blockchain enables the creation of smart contracts, with terms and conditions both sides can specify and that assure trust in the enforceability

of the contract and the identity of the counterparty. This system of distributed trust allows for lower transaction costs in the short term, but this

How Blockchain Works

A distributed database running on multiple servers continually checks the security and integrity of each transaction or data entry. Blocks chained by hash values and incentivized proof of work provide a foundation for distributed trust in blockchain.

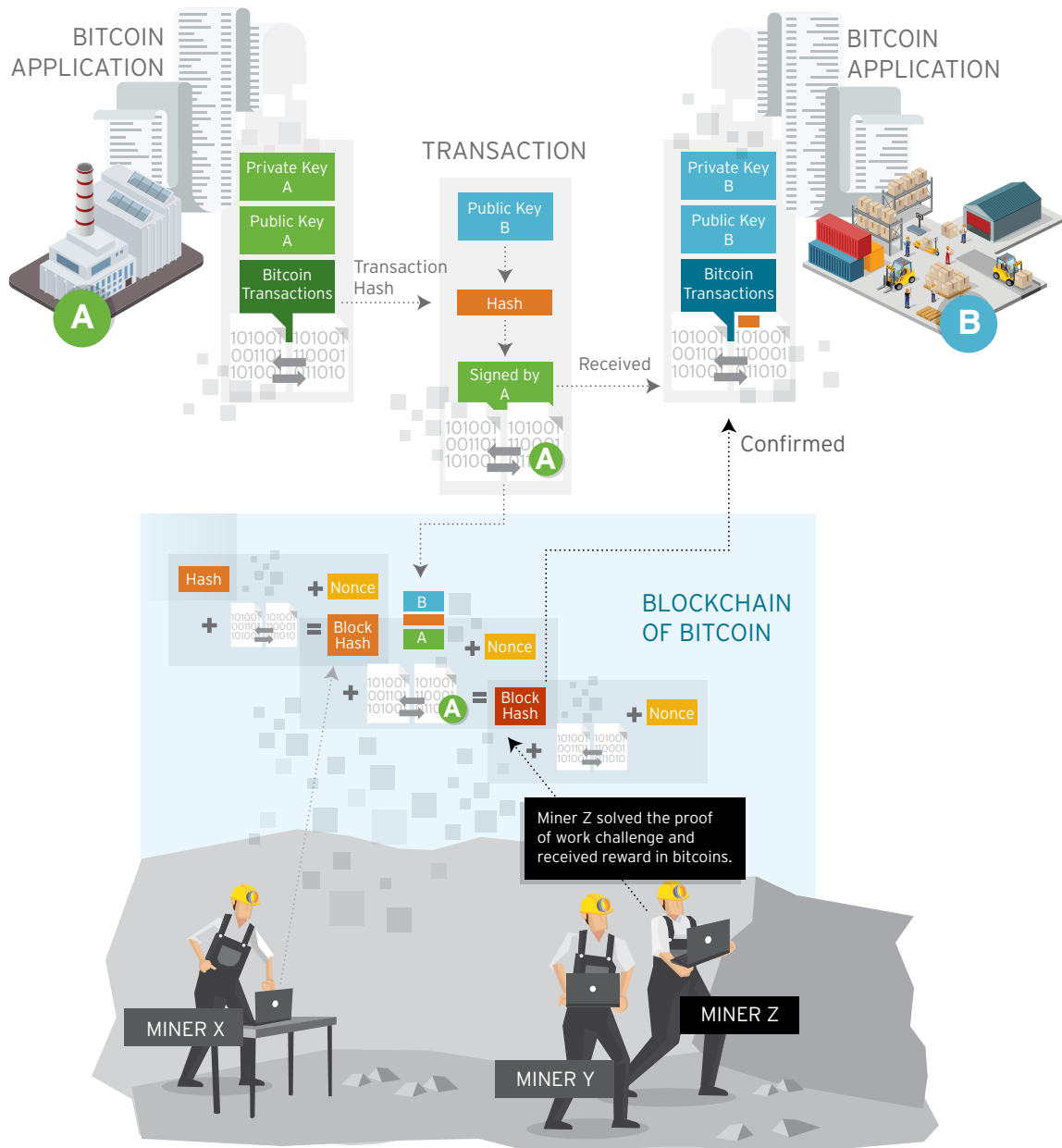


Figure 1

is just the beginning. In the long run it will enable more agile value chains, closer cooperation with business partners and faster integration with the Internet of Things (IoT), among other things.

Blockchain: A Deeper Dive

The initial objective of blockchain technology was to enable trusted financial transactions between any two parties without the need for a third party such as a bank. While it's best known in the financial services world, it can be used in any industry to enable faster, less expensive transactions and to support more agile supply chains that would be impossible otherwise.

When Satoshi Nakamoto introduced bitcoin in a white paper in 2008,¹ he did not use the term blockchain. But he laid the foundation for it by identifying the need to prevent "double spend" (two parties spending the same currency) without relying on a central trust authority such as a bank.

Solving this problem requires:

- Publicly "announcing" all transactions or changes to any of the currency, documents or transactions to all participants in a blockchain.
- Creating a system that allows all participants to agree on the transactions and their sequence.

It is the second requirement that gave birth to blockchain, a distributed database maintained by a series of servers. One server preserves a time stamp on all transactions on the blockchain. This server collects a set of transactions in blocks and publishes a hash (a unique set of numbers that, if changed, shows the data or transaction is invalid) for each block of transactions with a time stamp to verify their authenticity. As illustrated in Figure 1 (previous page), each owner of a transaction or document transfers the coin to the next owner by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the block.

However, that leaves the problem of how to ensure the validity of each block without a central authority to track all transactions. Blockchain solves this by providing an incentivized proof-of-work task for each participant. This process, called "mining," involves attempting to find a numerical value, known as a "nonce," that when combined with all open transactions in a block can be "hashed" into a value that satisfies a certain "difficulty" but is also easily verifiable. Once the nonce is found by a miner, the miner publishes the block with a hash to the rest of the peer-to-

peer network that makes up the blockchain. Other nodes accept the block, validate it and store it locally. The nodes then collect the next set of transactions and start another proof-of-work challenge. The node that solves the hashing challenge gets a reward in the form of bitcoins.

The blockchain concept has been extended over the last six years for use not only with currency but other types of records as well as smart applications that can conduct transactions independently. Innovations such as the Ethereum² platform for decentralized applications and the Hyperledger³ project to create a cross-industry open standard for distributed ledgers are making distributed, trusted and secure blockchain technology increasingly relevant for the manufacturing industry.

Blockchain in Manufacturing

The need for compressed product lifecycles has led to increased conflicts between manufacturers and suppliers. One particularly sensitive issue is managing the development and engineering of a complex product in a way that protects both the manufacturer's and supplier's competitive edge and differentiation. Other issues over the lifetime of a product, such as fixing the responsibility in automotive recalls, are made more difficult and expensive by the lack of trust between partners on both the transactional and strategic levels (see Quick Take, page 6).

Imagine a not-too-distant scenario where smart products on the IoT must securely run embedded software, and instantly and securely share massive amounts of data among those applications. These capabilities will add more tiers to the supply chain and dramatically increase the number of players and latency for root-cause analysis and corrective actions at the design level.

If the past is any indicator, the emerging complexity of products and business models will make a lack of trust an ever greater drag on manufacturing supply chains. Manufacturing organizations must spend large amounts of time, money and effort on negotiation, communications and paperwork to overcome this absence of trust. This is

The blockchain concept has been extended over the last six years for use not only with currency but other types of records as well as smart applications that can conduct transactions independently.

where the transformative power of blockchain lies, delivered by three critical capabilities:

Blockchain gives a trading partner immediate and low-cost trust in the identity and reputation of the counterparty in any financial or trading relationship.

- **Distributed integrity and reputation.** Blockchain gives a trading partner immediate and low-cost trust in the identity and reputation of the counterparty in any financial or trading relationship. This not only reduces the cost and time of transactions with known partners, but reduces the time and cost required to establish new business relationships. It also expands the universe of suppliers and customers for everything from raw materials to shipping and repair services, delivering quantum leaps in efficiency and agility.
- **Built-in monetary incentives to assure the security of every transaction and asset in the blockchain.** This allows blockchain technology to be used not only for transactions, but as a registry and inventory system for recording, tracking and monitoring all assets across multiple value chain partners. This secure information can range from information about raw materials or work-in-progress to intellectual property such as product specifications, purchase orders, warranty recalls or any currency or contract.
- **The ability to tap rules-based intelligence to perform business functions.** Blockchains enable the creation of intelligent, embedded and trusted program code, letting participants build terms, conditions and other logic into contracts and other transactions. It allows business partners to automatically monitor prices, delivery times and other conditions, and automatically negotiate and complete transactions in real time. This reduces transaction costs, maximizes efficiency and allows manufacturers to use data in different ways. It also opens the door for machine-to-machine transactions across the IoT.

These capabilities enable the transformation of a traditional supply chain, where transaction documents and contracts must be maintained by each partner's purchasing, accounting or legal department. With blockchain technology, all transactional elements are stored on decentralized computing nodes by various partners.

Two important examples of how blockchain can change manufacturing and logistics are:

- **Smart contracts:**⁴ A blockchain smart contract between a supplier and a buyer would consist not of a paper document in a drawer or a word processing document on a computer server. It would take the form of a computer program that runs on the blockchain and is executed by the entire blockchain network. Its program code – the terms and conditions of the contract – cannot be changed, and thus provides the trust that used to require elaborate control and audit processes. Not only can blockchain contracts contain the same level of detail as a physical contract, they can do something no conventional contract can: Perform tasks such as negotiating prices and monitoring inventory levels. This, again, replaces expensive, manual effort with automated, dynamic tracking of supply chains, inventory levels and prices to reduce costs and maximize profits.

To understand the potential of such smart contracts, think back to the “digital marketplaces” of the late 1990s and early 2000s. They served the role of a centralized trust and transaction processing hub which connected multiple supply chain partners. Blockchain technology can transform the vision of an “any-to-any” marketplace into reality. Imagine, for example, a commodity seller publishing a smart contract on a blockchain platform such as Ethereum that includes exact terms and conditions for product specifications, delivery and payment. Any buyer on the blockchain can find and act on the contract, acquire the needed product or service and pay for it without the processing overhead of the early digital marketplaces.

Any buyer on the blockchain can find and act on the contract, acquire the needed product or service and pay for it without the processing overhead of the early digital marketplaces.

- **Smart equipment and products:** Consider, for example, a smart vending machine that registers itself on a blockchain platform and tracks its own inventory and cash position. The machine will not only issue a replenishment order when it needs restocking, but can find the needed products at the best price, and order and pay for them without manual effort or the involvement of its owner. We believe this ability of smart machines to decentralize

Order-to-Cash Process with Smart Contracts

By providing trusted, automated transactions without the need for third parties, blockchain enables efficiency and agility wherever products, information or payments change hands.



Figure 2

decision-making and execution will bring a new era of efficiency to the manufacturing value chain. This concept is also relevant for IoT and machine-to-machine (M2M) integration using distributed blockchain technology.

As illustrated in Figure 2, a supplier or manufacturer issues a smart contract (Smart Contract 1, highlighted in light blue) on a blockchain including product definition, quantity, price, availability date as well as shipping and payment terms. A buyer looking for the product can use the blockchain to find the smart contract, verify the reputation of the supplier/manufacturer for quality and timeliness and complete the transaction. This replaces the more difficult and expensive manual processing required to issue a purchase order to the supplier.

Next, a supplier will search for a smart contract (Smart Contract 2, highlighted in gold) from a carrier with details such as “origination, destination, capacity, shipping conditions, carrier

fees and shipping time.” The supplier will accept the smart contract from the carrier. When the product is delivered to the buyer, the delivery confirmation will close Smart Contract 2 and the supplier will pay the carrier the shipping fees in cryptocurrency.

The delivery confirmation will also trigger a financial settlement in Smart Contract 1 between the supplier and buyer. In traditional supply chain processes, banks are used as the intermediary in the payments process. With smart contracts, the use of cryptocurrencies within blockchain will handle the settlement of funds.

The advantages of this approach include:

- **Low barriers to entry** for a supplier and a buyer to conduct the transaction.
- **The “reputation” of blockchain participants’ performance on past smart contracts** will help the highest-performing companies to demand premiums.

Quick Take

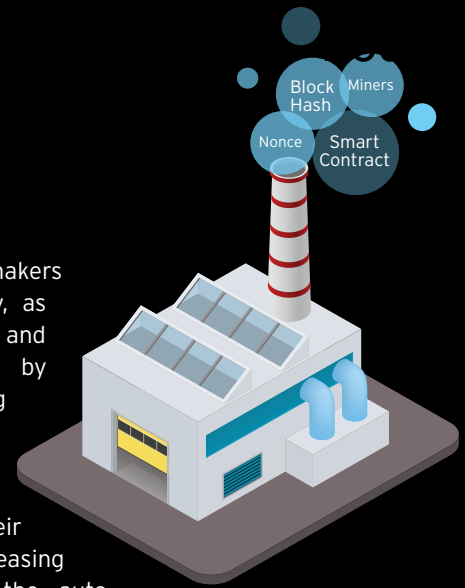
Blockchain in Manufacturing: The Art of the Possible

The applications of blockchain technology across the manufacturing space are endless. What follows are a few examples.

- **Audit trails:** Blockchain audit trails prove that a shirt was made in a factory paying a fair wage that provides good working conditions. This allows the retailer to charge a premium, the customer to feel good about the purchase and the workers to live better. Using blockchain audits to prove that organic food (or cage-free eggs) is genuine, for example, can help justify premium pricing, while fostering more humane/sustainable agriculture.
- **Real-time negotiation:** Intelligent blockchain contracts continuously query all other nodes in a blockchain for the best pricing, delivery times, and other terms and conditions for specialized aircraft engine parts. An engine manufacturer, for instance, can ramp up to meet demand more easily while cutting costs, while a smaller manufacturer can more easily fill demand from major customers.
- **Supply chain visibility and traceability:** Blockchain production records, for example, can trace which automobile airbags were made with an explosive compound that can cause

injuries or death. Automakers can reduce their liability, as well as their customer and vehicle tracking costs, by more quickly identifying the vehicles in which the airbags were used. Customers know more quickly whether their vehicle is affected, increasing their satisfaction with the auto brand and reducing their risk of injury or death.

- **Tapping data from IoT:** Easily tracked and authenticated blockchain data from IoT gives manufacturers more and better data about how their products perform over time, enabling them to improve quality. This also helps them move beyond production to more lucrative sales and services such as proactive replacement of failing parts.
- **IP management in product development:** Blockchain technology makes it easier and less expensive to securely share intellectual property such as designs, bills of material and production schedules among suppliers, manufacturers and shippers.



- **Smart equipment can replace human contracting parties for certain transactions**, as in our example of the vending machine.
- **Devices on the IoT can communicate with smart contracts to keep track of the status and state of smart contracts for settlements.** Smart shipping containers could, for example, automatically sell their surplus capacity.
- **Faster settlements** using cryptocurrencies.

Getting Ready for Blockchain

Manufacturing value chains are complex, multi-tiered combinations of various types of organizations providing design, sourcing, manufacturing, delivery and service across multiple geographies. Producing even a single component of a single product may involve a myriad of transactions, ranging from requests for quotes to the transmission of purchase orders and engineering change notices. Each transaction type may require dif-

ferent financial and regulatory intermediaries, as well as its own contract and trust relationship among the parties. The immediate and low-cost assurance of trust provided by blockchain technology can unleash disruptive innovation by allowing any supplier and any manufacturer to instantly find one another and begin a trading relationship.

So far, disruptive innovation in blockchain is being driven primarily by technology start-ups with a high tolerance for risk. Nonetheless, the overall trajectory of blockchain technology is extremely high (see Figure 3, next page). As a result, we

The immediate and low-cost assurance of trust provided by blockchain technology can unleash disruptive innovation by allowing any supplier and any manufacturer to instantly find one another and begin a trading relationship.

Pace of Blockchain Adoption

We expect the pace of blockchain's disruptive innovation to accelerate in the next 18 to 24 months.

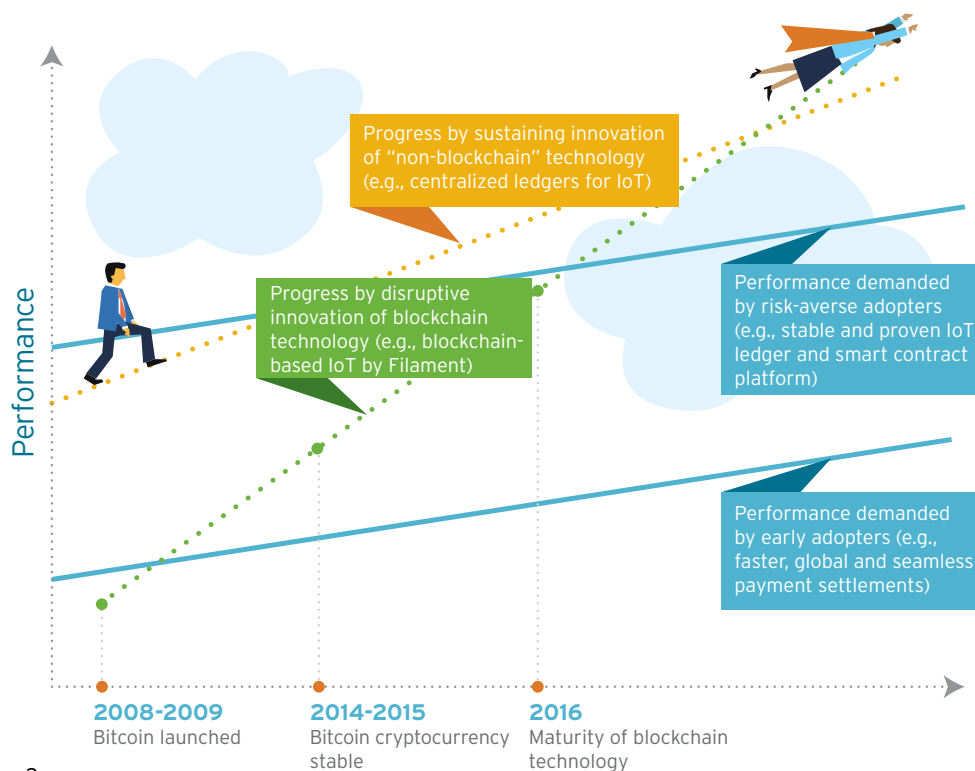


Figure 3

expect the next 12 to 18 months to be extremely important for companies looking to develop their blockchain innovation strategies.

As is typical with disruptive technologies, we recommend first executing proofs of concept to understand its potential and limitations, rather than measuring early deployments on their return on investment.

To help companies understand the relevance of blockchain smart contracts to them, and target their proofs of concept most effectively, we use two tools.

The first is the decision chart shown in Figure 4, next page, which helps identify areas where blockchain technology can deliver value.

One such area is in transactions where both parties lack trust in the definition and verification of a successful transaction. For example, Blockcharge⁵ uses blockchain technology to provide the authentication of users and billing for a peer-to-peer network of charging stations for electric vehicles without the need for a middle-man such as a bank.

A second useful tool to identify "low hanging fruit" blockchain opportunities is the functional complexity-automation capability framework shown in Figure 5 (next page), developed by authors and scholars Don and Alex Tapscott.⁶

Applying these two tools to the use of smart contracts in two manufacturing value chain transactions – the selling and purchasing of goods and services – produces a sound decision framework, as seen in Figure 6, page 9.

Challenges and Risks

Blockchain carries all the risks of any emerging technology. These range from the maturity of the technology itself to the standards surrounding it to the challenges of integrating it with existing platforms and business processes. The instant provision of trust among trading partners, and the ability of smart contracts to negotiate and finalize transactions, may require major changes in workflows and business processes.

Due to its disruptive nature, however, blockchain also carries two unusual risks potential adopters should monitor carefully.

Blockchain Smart Contract Relevancy Decision Chart for Manufacturing Value Chain Transactions

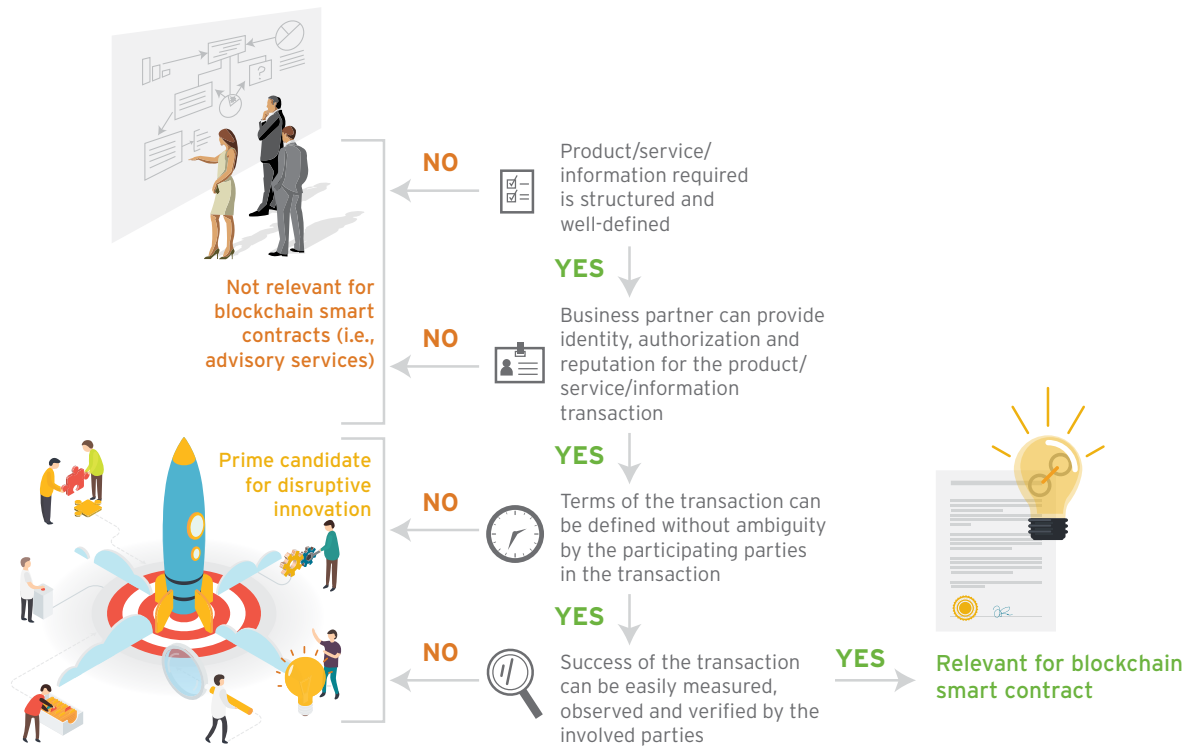
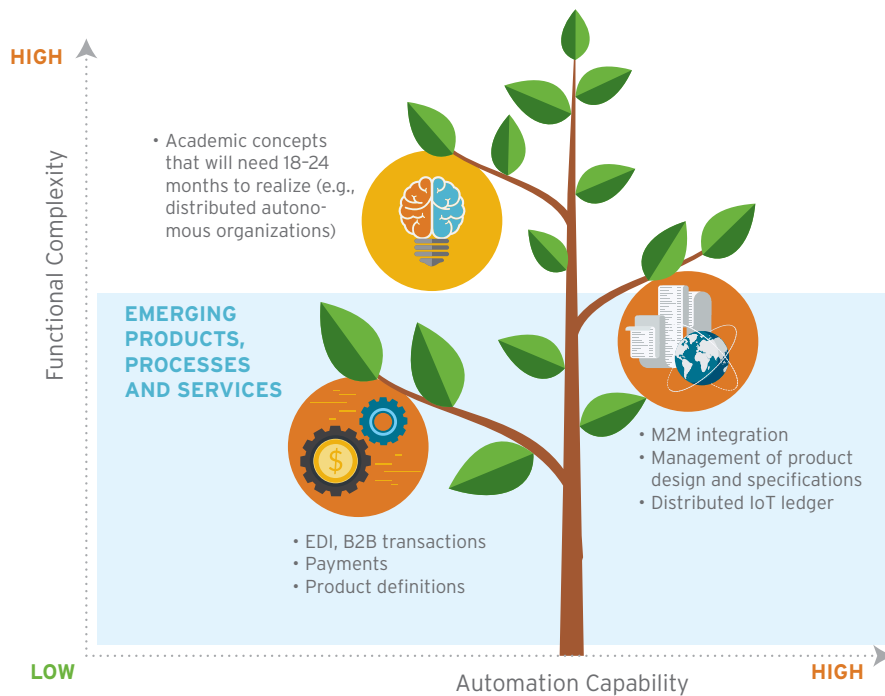


Figure 4

The Low-Hanging Fruit: Where to start with Blockchain Innovation



Source: Adapted from Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, by Don Tapscott and Alex Tapscott, Penguin Random House, June 2016.

Figure 5

Where Blockchain Works Best



Figure 6

- Government acceptance of or interference in blockchain peer-to-peer networks.** Many governments have not authorized the use of blockchain cryptocurrencies due to their lack of control over the monetary effects of cryptocurrencies and concerns over the criminal exploitation of the decentralized peer-to-peer network. When choosing blockchain opportunities, organizations should carefully consider where such lack of government acceptance would reduce or eliminate the value of blockchain in its value chains.
- Resistance from established players such as banks, exchange networks and other trust intermediaries could delay blockchain adoption.** Manufacturers may want to trial initial blockchain rollouts with smaller, newer “true digital” trading partners than larger partners unwilling to endanger their relationships with existing intermediaries.

Looking Forward

Blockchain isn’t just for banking and currency. Deployed correctly, its central benefit of rapid, easily established trust among trading partners can enable disruptive innovation in areas ranging from audit trails, real-time negotiation, supply chain visibility and tapping data from the IoT to managing intellectual property in product development. This trust can more quickly match

suppliers with the manufacturers that need their products, and slash the costs and delays associated with traditional accounting and vendor management.

But blockchain technology and standards are still emerging. Resistance from governments and existing intermediaries could slow its progress. As with any new technology, integrating blockchain with existing technologies and new platforms such as IoT, and adapting skills and business processes to it, will require investment.

Enterprises should proceed cautiously, with proofs of concept executed with partners, as they identify the “sweet spots” for this powerful new capability. We recommend that manufacturing companies do the following:

- Implement block chain technology evaluation and selective proofs of concept.
- Begin developing and testing innovative block chain business models and products.
- Leverage experienced partners to build a blockchain technology (hardware and software) lab to best understand the ever-changing potential and challenges.

Footnotes

- ¹ <https://bitcoin.org/bitcoin.pdf>
- ² www.ethereum.org/
- ³ www.hyperledger.org/
- ⁴ Nick Szabo, <http://szabo.best.vwh.net/smart.contracts.html>.
- ⁵ www.youtube.com/watch?v=OAOLqJ9oYNg
- ⁶ Don Tapscott & Alex Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*, Penguin Random House, June 2016, <http://blockchain-revolution.com/the-book/>.

About the Authors

Prasad Satyavolu is Global Head of Innovation within Cognizant's Manufacturing & Logistics business unit, where he focuses on the connected world (connected products, processes and infrastructure), including connected car and telematics services, IoT solutions for urban mobility and smart cities. He also focuses on customer fulfillment (integrated supply chain management that spans visibility planning and manufacturing execution) and general manufacturing industry challenges. Over the last 25-plus years, Prasad has held leadership roles in manufacturing and logistics and incubated a start-up in IT services and consulting that served the manufacturing industry. He holds an advanced degree in mechanical engineering from Dayalbagh Educational Institute, Dayalbagh, Agra, India, and completed a General Management Program (MEP) at Indian Institute of Management, Ahmedabad, India. He can be reached at Prasad.Satyavolu@cognizant.com.

Abhijeet Sangamnerkar is a Senior Business Transformation Leader and AVP within Cognizant's Manufacturing & Logistics business unit. He has over 20 years of consulting experience in the automotive, pharmaceuticals, chemicals and A&D industries. Abhijeet provides advisory services specializing in digital transformation strategy, business cases and roadmaps, and has managed several global transformation programs in the manufacturing industries. He holds an MBA from the Kellogg School of Management, Northwestern University, and a B.E. in electronics engineering from Gov't College of Engineering, Pune University, India. Abhijeet can be reached at Abhijeet.Sangamnerkar@cognizant.com.

About Cognizant

Cognizant (NASDAQ: CTSH) is a leading provider of information technology, consulting, and business process outsourcing services, dedicated to helping the world's leading companies build stronger businesses. Headquartered in Teaneck, New Jersey (U.S.), Cognizant combines a passion for client satisfaction, technology innovation, deep industry and business process expertise, and a global, collaborative workforce that embodies the future of work. With over 100 development and delivery centers worldwide and approximately 233,000 employees as of March 31, 2016, Cognizant is a member of the NASDAQ-100, the S&P 500, the Forbes Global 2000, and the Fortune 500 and is ranked among the top performing and fastest growing companies in the world. Visit us online at www.cognizant.com or follow us on [Twitter: Cognizant](#).



Cognizant

World Headquarters

500 Frank W. Burr Blvd.
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Fax: +1 201 801 0243
Toll Free: +1 888 937 3277
Email: inquiry@cognizant.com

European Headquarters

1 Kingdom Street
Paddington Central
London W2 6BD
Phone: +44 (0) 20 7297 7600
Fax: +44 (0) 20 7121 0102
Email: infouk@cognizant.com

India Operations Headquarters

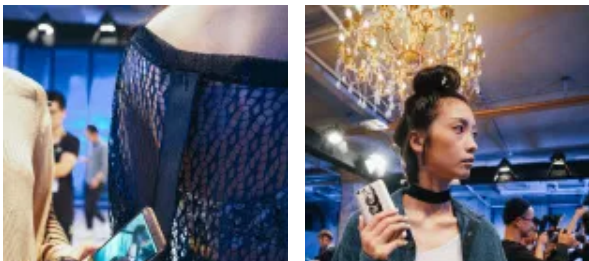
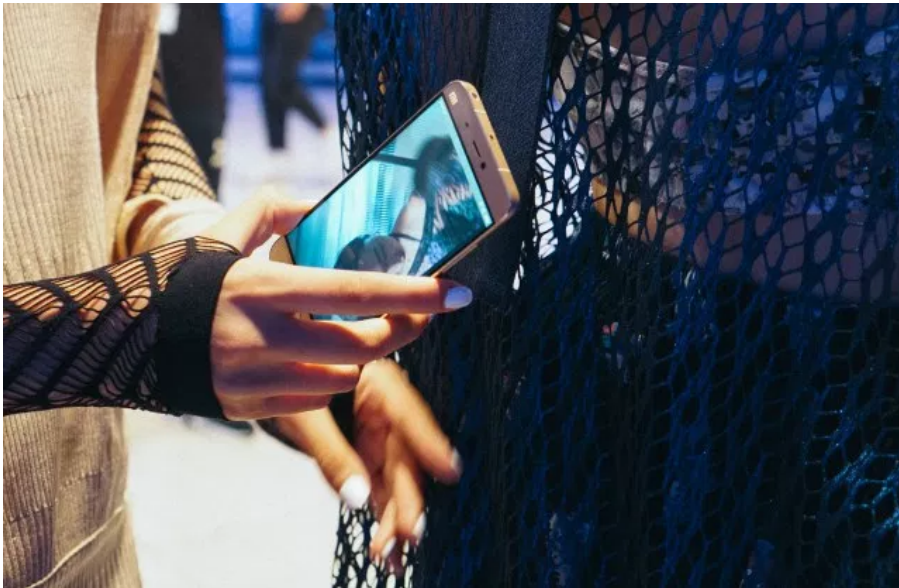
#5/535, Old Mahabalipuram Road
Okkiyam Pettai, Thoraipakkam
Chennai, 600 096 India
Phone: +91 (0) 44 4209 6000
Fax: +91 (0) 44 4209 6060
Email: inquiryindia@cognizant.com

BUSINESS / TECHNOLOGY

Indie Brand Babyghost Gets Techie With Scannable Clothes

Blockchain technology can help luxury brands to fight counterfeit products but Babyghost, launched six years ago by DVF alum Joshua Hupper and designer Qiaoran Huang, is using it as a next level marketing and customer relations tool.

By [Casey Hall](#) on January 11, 2017



SHANGHAI-Imagine scanning a jacket with a smartphone to watch a video.

That was the scene at the spring presentation of Babyghost, an indie fashion label based in [Shanghai](#) and [New York](#) with an effortless, urban vibe. The clothes, unveiled during [Shanghai Fashion Week](#) in October, were embedded with chips that could be scanned with smartphones to reveal exclusive content, like videos featuring the brand's "street kids", or influencers.

Blockchain technology can help luxury brands to fight counterfeit products but Babyghost, launched six years ago by [DVF](#) alum Joshua Hupper and designer Qiaoran Huang, is using it as a next level marketing and customer relations tool.

If people are familiar with blockchain at all, it's usually because of its role as a building block for digital currencies, such as bitcoin. In short, blockchain is an eco-system capable of recording and storing a unique digital coding of any product or content, whether it's bitcoin, a handbag or social media marketing campaign.

A physical fashion product may have its unique identity stored in a QR code, or encrypted chip embedded into the product itself, either of which can be scanned and verified on the blockchain network. Radio frequency identification [RFID] chips have already been adopted by luxury brands such as Salvatore Ferragamo and Moncler, but embedded blockchain chips offer brands far more than simply authentication.

Babyghost, with its ever-growing band of female millennial consumers, was quick to embrace social media platforms like Instagram and push out images and videos of Chinese It Girls like [Ju Xiaowen](#) and [Liu Wen](#) wearing its clothing. But Hupper was eager to take the brand to a new level from a technological standpoint.

"[Babyghost is] more of a community of people that wear it and Instagram and WeChat can only offer so much, I'm bored with it to be honest," he said.

So it was with interest that Huang and Hupper met with Shanghai-based blockchain company Bitse last summer, to discuss the potential for its VeChain (the name is a shortening of "verification blockchain") product for fashion brands.

“I’ve been interested in bitcoin since its inception, and our first conversation with VeChain happened when the Pokémon Go thing first came out, and the initial idea was that maybe you could collect the clothes and unreleased digital images or content like they were Pokémon,” Hupper said.

Bitse’s co-founder Sunny Lu is a former chief information officer of [Louis Vuitton](#) China and was immediately drawn to fashion industry uses for blockchain when he first heard about the burgeoning technology back in 2013.

“Anti-counterfeiting was the first step, but after a few months we started looking into other things. By building this unique ID for each product, you can do a lot of things with it,” Lu said.

“I can make an announcement to the network to say, I have ownership of this product, I own this bag or wallet, this is a key feature. We can put the chipset into the clothes and they are already in built with a story. This is about making each product unique and giving unique experiences to the clients.”

Multiple parties can contribute information to the encrypted chips, so for example, a raw materials manufacturer might be able to document the lifestyle of the cow that a particular piece of leather came from, manufacturers can add chapters to the story of how the leather was treated and a product constructed, then the finished product can be followed through the logistical chain to the hands of a consumer, who can claim ownership – whether the product is purchased from a store or on the second-hand market.

“For fashion and luxury, every brand wants to use their communications and or the product to connect with the customer. Most successful brands have done this successfully by utilizing Internet technology, but how do you go the next step, beyond apps, websites, social network platforms? The next step is developing individual connections between products and consumers,” Lu added.

Hupper highlighted the potential for brands to use the technology to continually update the information they provide to customers.

“More recently, we realized the content embedded in the blockchain can be updated, so you can scan your coat next month and it will bring up a new way of wearing it. Imagine being able to constantly educate your customer with a fresh way of looking at the same garment. This is the coolest wearable tech in history,” he said.

As the world’s capital of counterfeiting, it seems both counter-intuitive and sensible that China should be at the forefront of anti-counterfeiting technologies. And as the country where bitcoin has been embraced more enthusiastically than elsewhere and digital payment systems are the norm, perhaps it’s not a surprise that blockchain and other near field communication (NFC) technologies are taking off here.

In fact, blockchain is seen as such an important technology in China that the central government signaled it out as an area for development as part of its 13th five-year plan, which took effect last year and lasts until 2020.

“I think it’s huge, the amount of money that’s going into blockchain at the moment, it’s just incredible. There’s a tremendous amount of investment and the government has been really supportive,” said Zennon Kapron, founder of research and consultancy firm Kapronasia.

Even compared to a year ago, Sunny Lu and Bitse are finding a much more receptive audience to their products, as blockchain enters what Zennon Kapron dubs the “sexy new technology” section of the hype cycle.

“People are now chasing after this technology, they might not understand what they want to do with it, but they want to know what they can do with it,” Lu said.

“Before, [luxury brands like Louis Vuitton] could tell one story to everybody and then cross their fingers and hope that it impacts a certain percentage of the people hearing it. The next step is about brands interacting one-on-one with the client, blockchain can really help achieve this.”

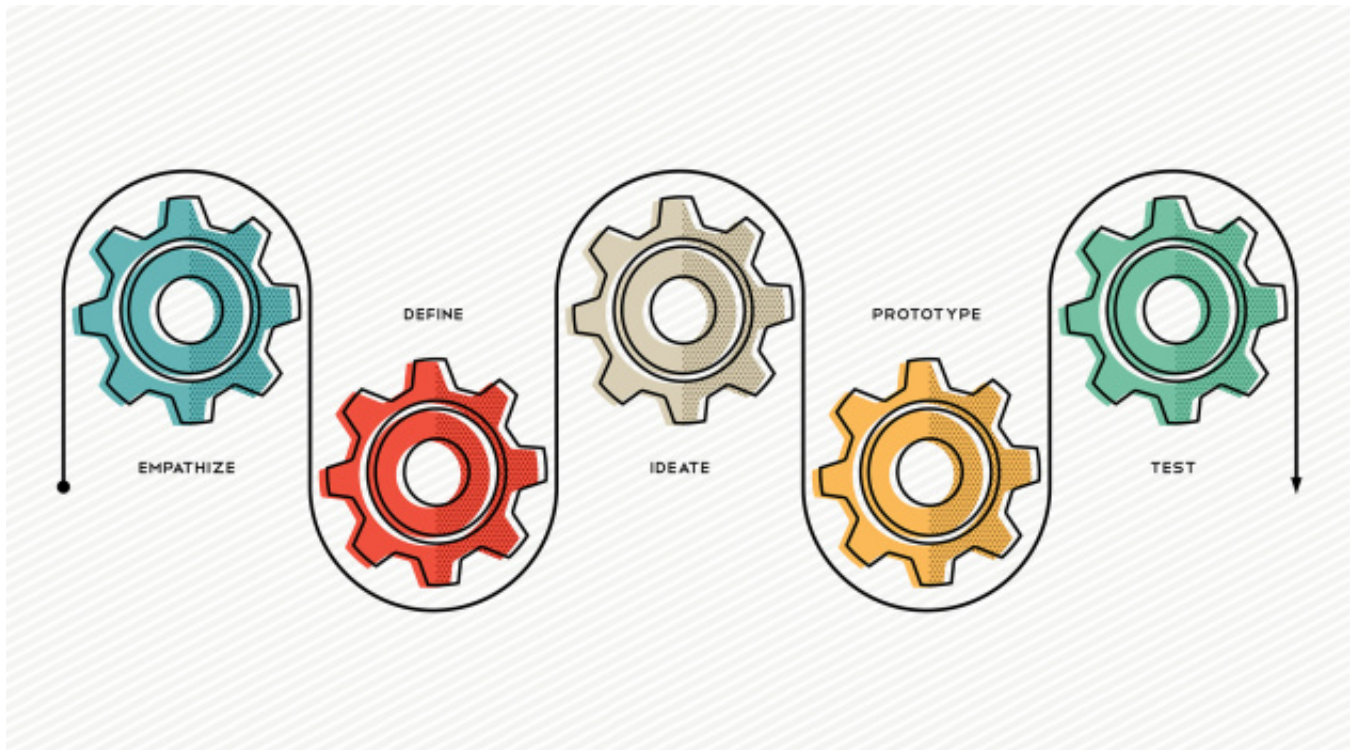
OP ED

Op-Ed | To Build Successful Businesses, Start Solving Problems

BY ARI BLOOM

JUNE 28, 2016 14:30

Like their counterparts in Silicon Valley, fashion entrepreneurs should begin by identifying real problems. Not enough dresses and handbags to choose from isn't one of them, argues Ari Bloom.



SAN FRANCISCO, United States — When I lived in New York, I met with a diverse range of talented fashion designers every week. Many of these individuals were actively

working to launch or grow a new brand, and it was staggering how each one would, without fail, tell me that they were doing something “nobody” else was. This always made me laugh. If you are a fashion designer, there are actually *a lot* of people doing *exactly* the same thing you are — namely, designing and producing non-essential clothing or accessories for people with finite disposable income and near infinite choices.

For the past 18 months, I’ve been working in Silicon Valley, where I am the chief executive of a retail technology company. Though I still actively work within the fashion industry and continue to mentor young designers through the CFDA Fashion Incubator, I now spend most of my days meeting with Sand Hill Road VCs, managing highly technical engineers and reviewing software and product roadmaps. Not surprisingly, this has changed my perspective completely on how to build both great products and successful companies. And while there have been many eye-opening lessons, the single most impactful thing I’ve learned is the power of what is commonly referred to as “design thinking.” This straightforward philosophy involves two simple steps: define a problem and then design a product that solves the problem. It has been championed for years by the Stanford School of Design, and has been successfully utilised by tech entrepreneurs and innovation experts like IDEO.

From my very first weeks working in tech, I started to experience how design thinking helped tech leaders approach building their companies and operating on a day-to-day basis. A tech entrepreneur might present their new company by identifying a multi-billion dollar solution to a problem or pain point in the world. A chief executive would challenge a proposed company strategy by overtly asking their team what problem it solved. A chief technology officer would build a product roadmap that first identified the meta problem and then prioritised the team’s work into short “sprints” to help build testable solutions within the larger framework that could be iterated from minimum viability into market ready product.

At the same time, as I continued to meet with fashion designers and executives at all

levels, I started to see a stark difference between the two industries. Fashion people continued to describe to me how their dresses or handbags were “different” or “better.” They didn’t identify, let alone solve, any problems. For the record, women don’t have the problem of not enough dresses to choose from and they certainly don’t lack for handbag options.

But this is not to say there aren’t problems that fashion can solve. Juicy Couture is actually a surprisingly poignant example here. When this brand hit the market, women clearly had a problem finding comfortable leisurewear that still made them feel sexy. Whether it set out to solve that problem or not, Juicy Couture succeeded because it convinced enough customers that it was the best solution available in the market. Companies like Spanx, Lululemon and Seven For All Mankind could all be said to have solved real problems in the fashion market.

It’s also important for fashion entrepreneurs to look for opportunities that exist beyond delivering great product and think about solving problems with how fashion is discovered and delivered. I can vividly remember attending one of the annual CFDA Fashion Incubator “business plan pitch contests” a few years ago. One of the judges patiently sat through all 10 presentations and then proceeded to admonish the designers for all doing “the same thing.” They were all talented and smart, and their products were beautiful, but nobody was presenting an innovative business model that solved a problem for the industry or consumers. Companies like Stitch Fix, Trunk Club, Birch Box and even Amazon are all great examples of companies that have solved real problems in retail and fashion. They are creating models and products that solve customer problems related to discovery, convenience and customisation.

Brands with a social mission also work within this framework. TOMS identified a problem in the world (lack of shoes in developing countries) and created a brand that lets customers be a part of the solution by buying product. In fact, it’s actually a double solution. The brand addresses the customer’s desire to help those in need and also their wish to feel good about the purchases they make. You can see this pattern taking

hold with companies like Everlane and Warby Parker as well.

It's no secret that fashion, just like any other industry, needs real innovation. Tomorrow's leaders will need to adopt an empathetic approach to see the situation clearly. Instead of simply launching traditional product companies that they think are "better" than what already exists, they should be looking hard at what problems exist in the world. They must then focus their attention on creating both products and business models that aim to actually solve these problems for customers.

Ari Bloom is the CEO of Avametric, a San Francisco-based fashion & retail technology firm.

The views expressed in Op-Ed pieces are those of the author and do not necessarily reflect the views of [The Business of Fashion](#).

Demystifying Fashion Labs: How Tech Is Changing The Way We Dress And Shop

What exactly is a fashion lab? A brief explainer.



[Carey Dunne](#) 07.16.14 12:59 PM

You may have heard the term "fashion lab" thrown around in the tech blogosphere lately. Perhaps it conjures images of shoes being grown in test tubes, or scientists in super stylish lab coats. What, exactly, is a fashion lab, and why should you care? Here's an explainer on how more and more engineers and retailers are using tech to change the way we dress and shop.

What are fashion labs?

The way we shop and dress ourselves increasingly relies on the digital: think e-commerce platforms like [Stylelect](#) (the Tinder for shoes), [ASAP54's app](#) that hunts down cool boots you saw on the subway, or [ThirdLove's bra-sizing app](#). Major retailers and designers are seeking to capitalize on this intersection between fashion and tech, and they're collaborating with engineers in incubator or accelerator programs, labeled "fashion labs." These programs, often made up of clusters of startups, aim to grow a new generation of brands from online roots, in hopes that a geeky environment will spawn the next cutting-edge digital platform in the fashion space. The definition of labs, accelerators, and incubators varies depending on whom you ask, but as Enrico Beltrami, a former Gucci corporate executive and founder of the [Fashion Technology Accelerator](#), told [Women's Wear Daily](#), "It's all part of the same trend. . . . We all want the same thing: to innovate fashion through technology."

What do they do?

Today, an online fashion company built five years ago can have a bigger valuation than an offline fashion company that has been around for 30 years.



Fashion labs are made up of employees savvy about iOS app development, cloud computing, and predictive analytics, not just about style and business—so that the retail brands they're attached to can compete with innovators at big tech companies. The labs create a variety of tech-based products—such as apps, digital storefronts, and wearable devices—related to fashion. Walmart's @Walmartlabs, started in 2011, and Nordstrom's Innovation Lab are examples of some of the bigger brands' internal labs. @Walmartlabs, for example, created an iPad app to help customers find the best pair of sunglasses for their face (it involved lots of selfies), and they're currently working on e-receipts—a way for customers to create shopping lists and track spending. Shopping center giant Westfield Group's Westfield Labs, based in San Francisco, has recently piloted digital storefronts, allowing customers at a California mall to browse items on a wall-sized touch screen pad, and a same-day delivery service powered by Silicon Valley startup Deliv. Such tech-minded fashion companies have an edge over less web-savvy retailers, or so the thinking goes: "Today, an online fashion company built five years ago can have a bigger valuation than an offline fashion company that has been around for 30 years," Beltramini said.

Who is involved in fashion labs?

In addition to Walmart and Nordstrom, major retail chains like American Eagle Outfitters Inc., Sears Holdings Corp., Target Corp., and Kohl's Corp have built their own internal tech labs. These retailers acquire tech startups—Walmart's has so far acquired 13—so that they can be the first to launch and benefit off a given innovation. Then there's the recently launched [New York Fashion Tech Lab](#), in which brands like J.Crew, Ralph Lauren, Macy's, and Kate Spade are mentoring fashion tech startups, helping them grow their ideas and apply them to retail. And software companies are pouring more resources into fashion—the German software giant SAP (Systems, Applications, and Products), for example, has launched a Silicon Valley-based lab, called AppHaus, which is piloting an app called MyRunway.

Who knew that the geeks and hip fashion kids would one day sit at the same cafeteria table?

Introducing BESPOKE

Lindsey Thomas October 10, 2014



Westfield Corporation has always been at the forefront of rethinking the retail space – in fact, that’s how Westfield Labs was born! Since establishing Westfield Labs two years ago with the sole purpose of innovating the retail ecosystem, Westfield has continued to explore the convergence of physical and digital, especially as relates to building new fully immersive and highly interactive experiences in our centers. It’s from this foundation that Westfield Corp and Labs came up with BESPOKE at Westfield San Francisco Centre. BESPOKE is a place that provides coworking, event and technology demo spaces all under one roof (well, under one *Dome* actually) in the center of downtown where the quintessential tech marketplace of San Francisco brushes against the retail district.

On the week of our 2nd anniversary, we’re excited to introduce BESPOKE!

With an eye for retail, and a heart for tech, we wanted to create a place where fashion runway shows and hackathons could happen side by side. We designed a beautiful event space fully customizable to the huge range of events that are quintessentially San Francisco. To open doors for unexpected synergies and collaborations, experimentation and integration, we’ll have a completely fresh coworking space right across the hall. Keeping in mind the great inspiration our own Westfield Labs team has found working inside the mall with customers right outside our door, we knew that building a coworking space inside the iconic Westfield San Francisco Centre created a unique offering that does not yet exist. Not to mention that Westfield San Francisco Centre is home to more than 20 million annual visitors and a built-in network of more than 200 established retailers and restaurants. We also wanted to give our visitors a chance to get in on the fun, so we incorporated a tech demo space where you can see, feel, and experience first-hand the true tech culture of San Francisco. In this space, we envision showcasing and demonstrating some of the hottest new technologies before anyone else can get their hands on it.

State-of-the-art technology, carefully thought out design elements, and the excellence and class you’ve come to expect from Westfield will make BESPOKE a new and unique place, and we’re very excited to be introducing the plans! This new ecosystem, where the San Francisco community can work, create, refine, showcase, entertain, play and sell all under one roof – is set to open in Spring 2015 and we’ll be sure to share more details as the spaces come to fruition! Check out www.bespokesf.co, and stay tuned to twitter.com/bespoke_sf for more details and drop us a line if you’re interested in learning how you can get involved.

Can Everlane Really Become the Next J.Crew?

[Chavie Lieber](#) Oct 8, 2015

In the last 12 months, Everlane has sold almost 30,000 pairs of shoes. That's a lot, considering the four-year-old e-commerce startup doesn't advertise and has no brick-and-mortar stores. But given the success of its [prized loafer](#), as well as its [street shoe](#), it's no surprise that the San Francisco-based brand plans to press even further in footwear, coming out with boots later this month. Wool winter coats are next on the docket.

The strategy, as it's been from the beginning, is for Everlane to keep slowly rolling out classic products that deeply resonate with its growing list of customers.

"We make products that are timeless in look," explains Everlane's CEO Michael Preysman. "The clothing has a current point of view, but can also be worn in 10 years. It's a very tricky thing to pull off. In our view, the best way to be environmentally sustainable is to create really great quality clothing that lasts and that has a lasting timestamp."

Everlane officially launched in 2011, after raising \$1.1 million from investors, with a simple cotton tee. It now stocks nearly 200 different items, and sells tens of thousands of that same T-shirt every month.

The brand has found its niche producing simple basics — button-down shirts, V-neck sweaters, trousers both slim and slouchy — in androgynous cuts, uncomplicated fabrics, and neutral colors. In stark contrast to fast-fashion behemoths that produce wastefully and under mysterious conditions, Everlane also gives shoppers a full snapshot of how and where its clothing is made.



Photo: Everlane

Now the company is in growth mode. In August, it [tapped](#) Rebekka Bay, the former Gap creative director tasked with fixing the [troubled retailer](#) only to have her role [eliminated](#), to lead Everlane's product and design teams. A few weeks ago, it sent out an email blast announcing it was looking to fill almost 20 new positions in its design, creative, engineering, and marketing departments — a bold move for a company that only has 70 existing employees.

If, as many believe, Everlane is on its way to becoming the next J.Crew, this expansion phase will be crucial to its success, if not its survival.

The Everlane [silk short-sleeve dress](#) is just the right amount of understated and luxurious. The fabric (100 percent crepe de chine) is soft but substantial, delicate enough to create a billowing silhouette, but not too thin or slippery as to feel cheap. Brands like Uniqlo and A.P.C. make similar dresses; Uniqlo's version is made of material many steps down in quality, while A.P.C.'s is four times Everlane's price.

"Retail isn't a space where there's a lot of information. You don't know where your clothing is made or what it costs to make."

Everlane's dress also comes with lots and lots of context. On the site, the piece's production costs are [broken down](#) — \$22.17 for materials, \$12.39 for labor, \$2.99 for duties — as is the markup. The dress costs \$38 to make and would be sold for \$190 at comparable retailers; Everlane charges \$98. The site also has a rundown of the [Hangzhou, China factory](#) where the dress was made, complete with photos of the factory's workers and the facility's interior.

"Retail isn't a space where there's a lot of information," says Preysman. "It's very obfuscated. You don't know where your clothing is made or what it costs to make. You pay a price for something and you have no idea why. So that's how we went about it, with a real inspiration to change the way retail works."

Ethical sourcing and competitive pricing is all part of what the brand calls "radical transparency," which has helped earn Everlane a cult following and a 200 percent sales increase last year alone.

Preysman says Everlane is able to cut down on its costs so it can price products lower than traditional retailers by cutting out the middleman. Everlane does all of its design in-house and works directly with factories; this is how it's able to charge, say, \$128 for [cashmere sweaters](#) instead of \$245. Everlane now works with 14 factories in five countries and visits new facilities constantly to determine if potential partners align with the company's ethical mandate.



Photo: Everlane

"We were looking at a new factory in China to produce our new line of close-to-body stretch cotton wear and it was a total nightmare," Preysman says of a recent compliance trip. "Clothes are all over the floor, people are sitting on little chairs, bent over for nine hours a day with hunchbacks because they've been sitting like this for years. That's when we say, 'Okay, there's no way we can work with this factory.' Even if other brands are using them, we won't produce there."

Rachel Krautkremer, an editorial director with creative agency Deep Focus, explains this element of Everlane's success thusly: Millennial shoppers care about pricing first and ethics second, so when Everlane offers similar clothing to J.Crew at a slightly cheaper price and makes its sustainability efforts known, it becomes an easy buy.

"Sixty-four percent of millennials would rather wear a socially-conscious brand than a luxury brand," she says. "It's a shift in how this generation views their clothing. They want to know where their product is coming from."



Photo: Everlane

This is a factor that has not been lost on the fast-fashion sector. Jeff Trexler, the associate director of Fordham's [Fashion Law Institute](#), notes brands like H&M and [Forever 21](#) have touted more ethical initiatives as of late. H&M just [announced](#) a \$1 million prize to whoever comes up with a way to help it reduce waste and pollution; Forever 21 [made plenty of noise](#) about the installation of solar panels in its LA headquarters last year.

"All of this is in direct response to Everlane's presence," Trexler posits. "Everlane has photos of smiling employees and clean factories abroad, and they are putting pressure on brands to follow suit, because otherwise it looks like they are hiding something."

Like many of its peers ([Bonobos](#), Warby Parker), Everlane chose to launch its brand online in an effort to further cut down on standard retail expenses. But as Sucharita Mulpuru, an analyst at market research firm Forrester, notes, e-commerce has become more competitive than ever: "There are 8,000 places to buy a T-shirt online!" Everlane, however improbably, has managed to stake its own claim on a segment of the market.

According to *The Economist*, Everlane had 350,000 members signed up for its email newsletter as of 2012. Earlier this year, when the brand offered pants on its site for the first time, it had a 12,000-person waitlist. Most of its exposure has come from social media; Everlane heavily promotes itself on Tumblr and Instagram.

"I haven't seen a brand grow this fast in a really long time," says Brian Sugar, one of Everlane's investors and board members. "Making a brand like Everlane is like capturing lightning in a bottle."

Everlane doesn't release collections by season, but instead introduces products one by one, with a small run of a new item appearing on the site a few times a year. This allows Everlane's design team to incubate an idea slowly, execute it with one prototype, and test it on customers before releasing larger editions.

"I haven't seen a brand grow this fast in a really long time. Making a brand like Everlane is like capturing lightning in a bottle."

"We're a living assortment, constantly editing the line and adding new product that builds on what we have and is relevant to the current cultural trends," says Preysman. "We expand what's working and lightly test what we don't do already. It's a multi-year process because we want to make sure the category works and resonates with our customer. We just launched the [Everlane Trench](#) and it was a huge hit. We started with a fabric and an idea based off our [Swing Trench](#), then built it out once there was success."

"There is always a story built around every new product," says Nick Brown, an investor in Everlane with New York City-based venture capital firm 14W. "That takes time and effort. They think about everything before something is released. They think about where it's position will be, whether customers need it, and if they'll respond to it. The design team takes their time figuring this all out because it takes a lot of time to do this well."

While Everlane doesn't have the same robust assortment as its competitors, Krautkremer says this is a conscious preference of the typical Everlane shopper and reflects the appetite of many consumers today: "People really like the convenience they offer. They like that they can sign onto the site and pick from a select few T-shirts and pants. It's not choice-overload, like with the Gap or J.Crew."

Julie Zerbo, the blogger behind watchdog site [The Fashion Law](#), believes Everlane was also one of the first brands to execute ethical fashion in a way that didn't compromise style. It helps that Everlane's rise dovetailed with the emergence of so-called [normcore fashion](#).



Photo: Everlane

"They do a good job at beating the stigma that ethically-made clothing has to be weird and made out of hemp for hippies," says Zerbo. "They do a really good job making it appealing without being too trendy to the point where people who buy their clothes become jaded with it after each season. They teach about simplicity and building a wardrobe of basics."

Zerbo adds Everlane has become a retailer shoppers can trust, one reason being that the clothing never goes on sale.

"We don't want to play games with anyone, because in traditional retail, brands sell 80 percent of their stuff at discount and it's really just them lying to their customer," echoes Preysman. "Our view is that we want to keep things as simple as possible for people. Wouldn't it be nice if you can go to a place and know that tomorrow and today, eight weeks from now, it's always the same price?"

"They do a good job at beating the stigma that ethically-made clothing has to be weird and made out of hemp for hippies."

A focus on the customer experience has also helped Everlane get ahead. The company has invested in technology to make its shopping experience more seamless. In March, it [announced](#) it was working with Facebook Messenger to connect directly with customers; in July, it debuted a dual shopping and weather [iPhone app](#).

"They have very thorough sizing information on their site and they treat customers really well," Ariella Major, a 25-year-old marketing associate and Everlane devotee, says. "Their marketing emails are very inviting and they send you really nice personal emails too. You can tell a thoughtful person wrote it."

Last year alone, Everlane's gross profits jumped from \$8.1 million to \$18 million, according to numbers compiled by PrivCo. Its revenue tripled in that same time, soaring from \$12 million in 2013 to \$36 million in 2014. (Everlane would not confirm these numbers nor would it disclose any additional financial information.) According to Sugar, "Everlane is marching down the path of becoming the next iconic American brand."

But for all its talk of transparency, Everlane is extremely tightlipped about internal goings-on. Preysman was the only Everlane employee offered up for this story, and no one from the design or creative teams was made available to be interviewed. Repeated requests to visit the brand's New York office were declined.



Photo: Everlane

Though Preysman wouldn't share future plans for expansion or customer acquisition, Everlane's recent hiring push hints at a desire to contend with big-name brands.

"It seems like they are positioning themselves to eventually compete against retailers like J.Crew and the Gap, and I think they can," says Zerbo. "J.Crew has gotten too expensive and fashion-y, and Gap has just descended down the ladder in terms of the desirability of young professionals."

Everlane, however, has a ways to go before it can stand up to these multi-billion-dollar brands. Preysman says the company has no plans to open brick-and-mortar stores and admits that the company has yet to see a profit.

"Without cash in the bank, you can't invest in the future of the company," he says. "Profit will be good to move the business forward, but we're not in it yet. In retail, it's generally quite challenging to start profiting until your company is really big."

Visibility is also a factor. While Preysman maintains he doesn't believe Everlane needs to be more aggressive in terms of consumer exposure, experts disagree. Right now, Everlane doesn't advertise — "it hasn't proven to be the most effective way to spend our time or money" — and only sends sporadic promotional mailers to current shoppers. Preysman says this strategy has worked for the company so far, but Forrester's Mulpuru underlines a simple fact: "Once they've hit everyone who's interested in Everlane, there's nowhere else to go."

Analysts are also worried the brand, like many that have come before it, may have a hard time scaling. Brown, of 14W, says the brand's biggest challenge is "to capitalize on the moment Everlane is having by fueling the business without growing too quickly."

"A lot of these companies that come out of the venture capital mill believe they can create a business and hit a homerun by expanding, when really, you're just launching a suicide bomb," muses Mulpuru. "It's a distorted way of thinking and is a product of Silicon Valley and other venture capitalists coming into the retail space who don't know retail behavior. Sometimes being small and special is a good place to be."

INTELLIGENCE

Is There Still Hope for Fashion Crowdfunding?

BY LAUREN SHERMAN

NOVEMBER 26, 2015 18:48

With new equity crowdfunding regulations now in place, some fashion labels and platforms see new potential in the model.



NEW YORK, United States — Since founding denim and basics brand DSTLD in 2013, Mark Lynn and Corey Epstein have raised \$4.3 million the old-fashioned way, turning to venture capitalists including CAA Ventures and Wavemaker Partners.

In the past year, DSTLD's sales have increased by 640 percent to more than 34,000 units. But to help fuel further growth, Lynn and Epstein needed to raise more capital. (As a direct-to-consumer label, customer acquisition is a critical — and expensive —

component of the business.) However, instead of turning once again to venture capital firms, the co-founders decided to launch a campaign on equity crowdfunding platform SeedInvest, which allows companies to raise money from Internet users.

For years, US regulations forbid non-accredited investors — those with a net worth of less than \$1 million and who earned less than \$200,000 annually in the last two years — from making equity investments in early stage companies, which are inherently risky, on the grounds of investor protection. (On popular crowdfunding sites like Kickstarter, people who contribute funds are rewarded with giveaways like t-shirts, but do not acquire equity in the companies they support.) But in June 2015, in response to criticism that ordinary investors were being locked out of the start-up boom, the US Securities and Exchange Commission (SEC) implemented Title IV of the JOBS Act, which, among other things, now allows non-accredited individuals to invest in early stage companies.

Lynn and Epstein posted their pitch on SeedInvest in September 2015 and, so far, DSTLD has received more than \$9.4 million worth of “indicated interest” from individual investors. Whether or not that interest turns into actual cash remains to be seen: not only do these would-be investors still need to make real commitments, but DSTLD still needs to determine just how much equity investors will receive. Nonetheless, Lynn is taken with the idea. “It’s an opportunity to turn the capital formation structure on its head,” he says. “It allows your best customers to participate in the brand story in a really profound way. They can be evangelisers of the product.”

It’s a powerful concept — but one that has rarely worked in practice for fashion labels aiming to crowdfund their growth. Indeed, while companies are projected to raise \$34.4 billion in crowdfunded investments in 2015, according to research and advisory firm Massolution, just a sliver of those using crowdfunding operate in the apparel sector. Of the 93,546 projects successfully funded on Kickstarter since the platform launched, only 3,163 (or 3 percent) have been fashion-related. And while the success rate of technology-related campaigns (20 percent) is actually lower than that of fashion-related campaigns (24 percent), technology projects have successfully raised a total of \$297 million, significantly more than the \$59 million raised by fashion projects.

But for many proponents of the approach, Title IV of the JOBS Act — and, more recently, Title III of the same regulation, passed by the SEC on October 30, which makes it even easier for early stage startups to raise money from non-accredited investors — have changed the prospects for crowdfunding in fashion.

To be sure, not everyone is pleased with the new rules. Companies wishing to raise under \$20 million will have to submit to review by US state governments and SeedInvest, for one, is concerned that these authorities will charge exorbitant fees and bottleneck the process. But the new rules, which are set to go into effect on January 29, 2016, have undoubtedly created new momentum for both crowdfunding platforms and individual companies aiming to crowdfund their expansion.

Fashion Fund, a Seattle-based crowdfunding platform, plans to launch on January 29, as soon as the new rules take effect. “In fashion, a designer may just need that ugly \$500,000 or \$800,000 to get off the ground,” says Fashion Fund founder and managing director Kartik Ram. The company will launch with brands including Glamster, which specialises in sleek bike wear, Triangl swimwear and Hare+Hart handbags. “Americans have a mindset to take risks,” Ram says. “There is such a propensity for hipster and artisan brands. Crowdfunding allows customers to become investors.”

Whether or not customers want to become investors, however, remains to be seen. Over the years, several companies have aimed to build go-to platforms for crowdfunded fashion, including Catwalk Genius (founded in 2007), FashionStake (2010), Cut on Your Bias (2012) and ZaoZao (2012). Each platform had a slightly different approach. London-based Catwalk Genius helped designers raise funds to finance new collections. Revenues from resulting sales were split equally between the “supporters,” the designer and the platform. In its first iteration, New York-based Fashion Stake rewarded supporters by offering clothing credits in what essentially amounted to pre-order. Cut On Your Bias, also based in New York, used a similar model, but asked supporters to vote on specific designs. Hong Kong-based ZaoZao took a similar approach, but focused on Asian designers.

But each of these firms has since shuttered or been absorbed by another company. Fab.com acquired FashionStake in 2012, although by that time the company had

already pivoted its business model away from crowdfunding to traditional e-commerce. ZaoZao also pivoted to traditional e-commerce before closing. And, despite early buzz, neither Catwalk Genius nor Cut On Your Bias ever really took off. What went wrong?

“The problem we were solving was that there was this growing group of independent designers — some professional and some not — that lacked a way to market their creations and grow their businesses. Initially, we focused on the second part of the problem by providing financing and customer feedback to designers pre-production, enabling them to make better bets on inventory,” explains FashionStake co-founder Daniel Gulati. “While this was a valid pain point, the more interesting business was around the first part: providing a distribution channel for designers to sell existing inventory. We noticed that within the first few months of launching and shifted the business quickly to capitalise.”

“Many of the people who came to our site didn’t quite know what crowdfunding was and a lot of our marketing efforts were spent explaining it to them,” says ZaoZao co-founder Vicky Wu. “We soon realised that we were never going to achieve the scale of a first mover like Kickstarter and that we were just adding more noise to the market.”

As for Cut On Your Bias, featuring designers who were known in the fashion industry but not to a broader audience — such as Timo Weiland or Suzanne Rae — was a significant barrier. “It was super difficult to gain customer trust,” says Louis Monoyudis, the company’s founder.

Often, the emerging designers crowdfunding their businesses are highly inexperienced. “When we review a project, the first thing we do is make sure that the designer has the ability to complete it,” says Lucas Vigliocco, co-founder of London-based fashion crowdfunding platform Wowcracy. “Many of the designers are not yet professionals, so we need to make sure that the person is committed to the project and our process.” While more than 1,250 designers have submitted projects to Wowcracy since it was founded in 2013, only 250 have actually been published by the site.

Many designers remain unprepared to produce what they've promised. "One thing that catches a lot of people off guard is how many unique items they're going to have to build," says Maxwell Salzberg, who runs BackerKit, a company making fulfillment software geared towards crowdfunded start-ups. "Even if you're making a belt in three different colors with three different buckles and three different sizes to choose from, that's [a lot] of SKUs."

What's more, the skill level and manufacturing know-how of young designers can vary wildly, making it difficult for many to deliver well-made garments at a competitive price point. "Even making a pattern is an investment," says Cecilia Pagkalinawan, who advises fashion start-ups. (Pagkalinawan also founded crowdsourced-fashion platform StyleTrek in 2010. It closed two years later.)

Returns, too, can be an albatross. Because most of the designers featured on crowdfunding sites are new, it's difficult for consumers to gauge accurate sizing, which can result in a high return rate. "Big fashion companies can afford to have free returns," Salzberg says. "If you're an independent brand, that can be a pretty big ding in your budget."

Yet there are fashion crowdfunding success stories, from Ministry of Supply, which raised \$430,000 for its sweat-wicking Apollo dress shirt on Kickstarter in 2012, to BauBax, the travel jacket that has attracted more than \$10 million on Indiegogo. Consider the case of Victor Athletics, the Cincinnati-based company that raised more than \$100,000 on Kickstarter to produce its Tennessee-made tees and sweatshirts. The proprietors already owned the upscale line Noble Denim — sold at stores such as Japan's Journal Standard — and were able to raise awareness through its network of followers. They also already had great relationships with manufacturers. Finally, "We did research around what price points were attractive to people and we chose the direct-to-consumer model so that we could keep the prices a bit lower," explains co-founder Abby Sutton. Victor Athletics' first round of sweatshirts are being shipped in early October and the company has plans to open its first physical store in Cincinnati later on this year.

Gulati believes that these wins for fashion crowdfunding indicate that independent

platforms such as Fashion Fund and Wowocracy could indeed succeed. “Although no one has built an independently huge business in the space, I think Kickstarter and others have shown that there is growing acceptance of the model,” he says. “Aside from the consumer behaviour trends, the other development is regulatory, where you see equity-based crowdfunding legislation really starting to take shape and in many regions, this legislation has been enacted,” Gulati continues. “If new startups are able to facilitate revenue share or equity deals between designers and their backers in a way that previously wasn’t allowed, there’s real breakout potential there.”

To be sure, venture capitalists themselves are not entirely turned off by the idea of fashion crowdfunding platforms. “I’m hoping that the advantages — zero waste, demand that comes before the supply, price control — will outweigh the slight negatives,” says Billy Draper of California-based seed-stage venture capital firm Draper Associates, which has invested in several specialised crowdfunding platforms including Indiegogo and UsTrendy. “When you pick one industry as your focal point, you learn a lot more about that industry.”

However, some of those who have been through it still aren’t convinced that selling fashion through crowdfunding will ever work. “The whole premise is based on putting the ball in the customer’s court. I hate to admit it, but fashion really is dictated by the influencers,” Wu says. “Most people are followers.”

New Rules Give Startups Access to Main Street Investors

Starting Monday, small companies can raise as much as \$1 million online from ordinary investors



Naval Ravikant, co-founder of AngelList, at an event in 2014. AngelList.com, which connects startups with wealthy investors, plans to work with Republic.co, a securities crowdfunding portal that is waiting for regulatory approval. Photo: Steve Jennings/Getty Images for TechCrunch

By Ruth Simon
May 11, 2016 3:42 p.m. ET

Small businesses will soon be able to sell shares to Main Street investors on crowdfunding portals, instead of trying to lure those backers with promises of T-shirts, coffee mugs or other merchandise.

Starting Monday, small companies and startups can raise as much as \$1 million online from ordinary investors in a 12-month period. Until now, federal securities laws allowed only wealthy individuals, or so-called accredited investors, to participate in such offerings. The new fundraising option stems from the 2012 Jumpstart Our Business Startups Act, or JOBS Act.

But even supporters of equity crowdfunding say it is likely to get off to a slow start, in part because of the complexity and newness of the process, higher costs and disclosure requirements.

Under the new rules, companies must raise money through a registered broker-dealer or a funding portal approved by regulators. Ten broker-dealers have told regulators they plan to participate, while more than 40 firms have applied to become portals, according to the Financial Industry Regulatory Authority, a self-regulatory group.

As of early Wednesday, Finra had approved five of these portal applications. Four applications have been withdrawn, according to the Securities and Exchange Commission. The others “are pending either the submission of required information or are just under review,” a Finra spokesman said.

Indiegogo Inc., a crowdfunding website, said it expects to move into securities offerings later this year. “Venture investment is natural evolution for a lot of our entrepreneurs,” said Indiegogo Chief Executive David Mandelbrot. “It’s the first time that all people can participate in that marketplace.”

AngelList.com, which connects startups with wealthy investors, plans to work with Republic.co, a securities crowdfunding portal that awaits regulatory approval and is expected to launch soon. “We...are going to create a seamless experience for companies that raise [money] on AngelList and then want to add a piece for the crowd after,” said AngelList co-founder Naval Ravikant.

Kickstarter, the largest rewards-based crowdfunding site, said it doesn’t plan to expand into securities offerings. “Our mission is to help bring creative projects to life,” a Kickstarter spokesman said. “Not all creative ideas are meant to be investment vehicles.”

Thirty-one states and the District of Columbia already [allow local firms to raise money from area residents](#), but few companies have taken advantage of the opportunity to tap into crowdfunding and bring on investors.

Some entrepreneurs are likely to balk at the idea of dealing with dozens or even hundreds of mom-and-pop investors, but the new approach could appeal to companies seeking to build close ties to potential customers.

“It provides access to money from people who are passionate about what you are doing,” said Paul LaPorte, chief executive of MF Fire Benefit LLC, a College Park, Md.-based maker of wood stoves that is considering using the new fundraising option. “It makes them perfect brand ambassadors and they can also be your customers.”

Under the rules, individuals with income or net worth of less than \$100,000 can invest the greater of \$2,000, or 5% of either their annual income or net worth, whichever is lower, in small-scale securities offerings in a 12-month period. Investors with income and net worth of at least \$100,000 can invest up to 10% of their annual income or net worth, whichever is lower.

But investors seeking the next Facebook or Uber should proceed with caution. “These are companies that are new or close to brand new and are speculative,” cautions Washington State Securities Administrator William Beatty. “You don’t want to invest more in any one company than you can afford to lose.” Even for successful companies, holding periods are likely to run five to seven years.

Entrepreneurs, meanwhile, face higher costs and stiffer requirements than if they raised money via Kickstarter. Companies, for instance, must spell out their financial condition and how they plan to use proceeds from the offering. Unlike firms raising money from wealthy investors, they must also publicly file annual financial statements that have been reviewed by an independent accountant or, in some cases, audited.

Fees will vary. NextSeed Inc. expects to charge 5% to 10% of the amount raised. SeedInvest LLC will charge a fee that is 5% of the amount raised and take a 5% equity stake. Wefunder Inc. plans to collect 3% from issuers and 2% from investors.

“I think it will be funding of last resort for many companies,” said Rory Eakin, founder of CircleUp Network Inc., which through its portal CircleUp helps consumer-goods companies raise money from wealthy investors and isn’t planning to operate under the new rules. “If you are a small consumer brand, you don’t want Wal-Mart to know how big you are and the profitability of your brand.”

Some entrepreneurs say the new rules could plug a gap in funding sources. “Access to resources and capital, in particular, is our biggest challenge,” said Bernard Loyd, president of Urban Juncture Inc., a community development firm working to revitalize Chicago’s Bronzeville neighborhood. “I believe there are people who would like to contribute to the revitalization of communities like this, but don’t have access to the information to do so.”



U.S. SECURITIES AND EXCHANGE COMMISSION

ABOUT DIVISIONS ENFORCEMENT REGULATION EDUCATION FILINGS NEWS

CORPORATION FINANCE

About

Accounting and Financial
Reporting Guidance

Compliance and
Disclosure
Interpretations

Filing Review Process

No-Action, Interpretive
and Exemptive Letters

Statutes, Rules and
Forms

Contact Us

Regulation Crowdfunding: A Small Entity Compliance Guide for Issuers^[1]

May 13, 2016

Table of Contents

This compliance guide is divided into the following parts:

1. [Introduction](#)
2. [Requirements of Regulation Crowdfunding](#)
3. [Issuer Disclosure](#)
4. [Limits on Advertising and Promoters](#)
5. [Restrictions on Resales](#)
6. [Exemption from Section 12\(g\)](#)
7. [Bad Actor Disqualification](#)
8. [Other Resources](#)
9. [Contacting the SEC Staff](#)

1. Introduction

Under the Securities Act of 1933, the offer and sale of securities must be registered unless an exemption from registration is available. Title III of the Jumpstart Our Business Startups (JOBS) Act of 2012 added Securities Act Section 4(a)(6) that provides an exemption from registration for certain crowdfunding transactions.^[2] In 2015, the Commission adopted [Regulation Crowdfunding](#) to implement the requirements of Title III.^[3] Under the rules, eligible companies will be allowed to raise capital using Regulation Crowdfunding starting May 16, 2016.

2. Requirements of Regulation Crowdfunding

In order to rely on the Regulation Crowdfunding exemption, certain requirements must be met.

a. Maximum Offering Amount of \$1 Million

A company issuing securities in reliance on Regulation Crowdfunding (an "issuer") is permitted to raise a maximum aggregate amount of \$1 million in a 12-month period. In determining the amount that may be sold in a particular offering, an issuer should count:

- the amount it has already sold (including amounts sold by entities controlled by, or under common control with, the issuer, as well as any amounts sold by any predecessor of the issuer) in reliance on Regulation Crowdfunding during the 12-month period preceding the expected date of sale, plus
- the amount the issuer intends to raise in reliance on Regulation Crowdfunding in this offering.

An issuer does not aggregate amounts sold in other exempt (non-crowdfunding) offerings during the preceding 12-month period for purposes of determining the amount that may be sold in a particular Regulation Crowdfunding offering.

b. Investors Subject to Limits

Individual investors are limited in the amounts they are allowed to invest in all Regulation Crowdfunding offerings over the course of a 12-month period:

- o If either of an investor's annual income or net worth is less than \$100,000, then the investor's investment limit is the greater of:
 - o \$2,000 or

- o 5 percent of the lesser of the investor's annual income or net worth.
- o If both annual income and net worth are equal to or more than \$100,000, then the investor's limit is 10 percent of the lesser of their annual income or net worth.
- o During the 12-month period, the aggregate amount of securities sold to an investor through all Regulation Crowdfunding offerings may not exceed \$100,000, regardless of the investor's annual income or net worth.

Spouses are allowed to calculate their net worth and annual income jointly. This chart illustrates a few examples of the investment limits:

Investor Annual Income	Investor Net Worth	Calculation	Investment Limit ^[4]
\$30,000	\$105,000	Greater of \$2,000 or 5% of \$30,000 (\$1,500)	\$2,000
\$150,000	\$80,000	Greater of \$2,000 or 5% of \$80,000 (\$4,000)	\$4,000
\$150,000	\$100,000	10% of \$100,000 (\$10,000)	\$10,000
\$200,000	\$900,000	10% of \$200,000 (\$20,000)	\$20,000
\$1,200,000	\$2,000,000	10% of \$1,200,000 (\$120,000), subject to \$100,000 cap	\$100,000

c. Transactions Conducted Through an Intermediary

Each Regulation Crowdfunding offering must be exclusively conducted through one online platform. The intermediary operating the platform must be a broker-dealer or a funding portal that is registered with the SEC and FINRA.

Issuers may rely on the efforts of the intermediary to determine that the aggregate amount of securities purchased by an investor does not cause the investor to exceed the investment limits, so long as the issuer does not have knowledge that the investor would exceed the investment limits as a result of purchasing securities in the issuer's offering.

d. Eligibility

Certain companies are not eligible to use the Regulation Crowdfunding exemption. These include:

- non-U.S. companies;
- companies that already are Exchange Act reporting companies;
- certain investment companies;
- companies that are disqualified under Regulation Crowdfunding's disqualification rules;
- companies that have failed to comply with the annual reporting requirements under Regulation Crowdfunding during the two years immediately preceding the filing of the offering statement; and
- companies that have no specific business plan or have indicated their business plan is to engage in a merger or acquisition with an unidentified company or companies.

3. Disclosure by Issuers

a. Form C

Any issuer conducting a Regulation Crowdfunding offering must electronically file its offering statement on [Form C](#) through the Commission's Electronic Data Gathering, Analysis and Retrieval (EDGAR) system and with the intermediary facilitating the crowdfunding offering. A Form C cover page will be generated when the issuer provides information in XML-based fillable text boxes on the EDGAR system. Other required disclosure that is not requested in the XML text boxes must be filed as attachments to Form C. There is not a specific presentation format required for the attachments to Form C; however, the form does include an optional "Question and Answer" format that issuers may use to provide the disclosures that are required but not included in the XML portion.

b. Offering Statement Disclosure

The instructions to Form C indicate the information that an issuer must disclose, including:

- information about officers, directors, and owners of 20 percent or more of the issuer;
- a description of the issuer's business and the use of proceeds from the offering;
- the price to the public of the securities or the method for determining the price,
- the target offering amount and the deadline to reach the target offering amount,
- whether the issuer will accept investments in excess of the target offering amount;
- certain related-party transactions; and
- a discussion of the issuer's financial condition and financial statements.

The financial statements requirements are based on the amount offered and sold in reliance on Regulation Crowdfunding within the preceding 12-month period:

- For issuers offering \$100,000 or less: Financial statements of the issuer and certain information from the issuer's federal income tax returns, both certified by the principal executive officer. If, however, financial statements of the issuer are available that have either been reviewed or audited by a public accountant that is independent of the issuer, the issuer must provide those financial statements instead and will not need to include the information reported on the federal income tax returns or the certification of the principal executive officer.
- Issuers offering more than \$100,000 but not more than \$500,000: Financial statements reviewed by a public accountant that is independent of the issuer. If, however, financial statements of the issuer are available that have been audited by a public accountant that is independent of the issuer, the issuer must provide those financial statements instead and will not need to include the reviewed financial statements.
- Issuers offering more than \$500,000:
 - For first-time Regulation Crowdfunding issuers: Financial statements reviewed by a public accountant that is independent of the issuer, unless financial statements of the issuer are available that have been audited by an independent auditor.
 - For issuers that have previously sold securities in reliance on Regulation Crowdfunding: Financial statements audited by a public accountant that is independent of the issuer.

c. Amendments to Offering Statement

For any offering that has not yet been completed or terminated, an issuer can file on Form C/A an amendment to its offering statement to disclose changes, additions or updates to information. An amendment is required for changes, additions or updates that are material, and in those required instances the issuer must reconfirm outstanding investment commitments within 5 business days, or the investor's commitment will be considered cancelled.

d. Progress Updates

An issuer must provide an update on its progress toward meeting the target offering amount within 5 business days after reaching 50% and 100% of its target offering amount. These updates will be filed on Form C-U. If the issuer will accept proceeds over the target offering amount, it also must file a final Form C-U reflecting the total amount of securities sold in the offering. If, however, the intermediary provides frequent updates on its platform regarding the progress of the issuer in meeting the target offering amount, then the issuer will need to file only a final Form C-U to disclose the total amount of securities sold in the offering.

e. Annual Reports

An issuer that sold securities in a Regulation Crowdfunding offering is required to provide an annual report on Form C-AR no later than 120 days after the end of its fiscal year. The report must be filed on EDGAR and posted on the issuer's website. The annual report requires information similar to what is required in the offering statement, although neither an audit nor a review of the financial statements is required. Issuers must comply with the annual reporting requirement until one of the following occurs:

- (1) the issuer is required to file reports under Exchange Act Sections 13(a) or 15(d);
- (2) the issuer has filed at least one annual report and has fewer than 300 holders of record;
- (3) the issuer has filed at least three annual reports and has total assets that do not

exceed \$10 million;

(4) the issuer or another party purchases or repurchases all of the securities issued pursuant to Regulation Crowdfunding, including any payment in full of debt securities or any complete redemption of redeemable securities; or

(5) the issuer liquidates or dissolves in accordance with state law.

Any issuer terminating its annual reporting obligations is required to file notice on Form C-TR reporting that it will no longer provide annual reports pursuant to the requirements of Regulation Crowdfunding.

4. Limits on Advertising and Promoters

An issuer may not advertise the terms of a Regulation Crowdfunding offering except in a notice that directs investors to the intermediary's platform and includes no more than the following information:

(a) a statement that the issuer is conducting an offering pursuant to Section 4(a)(6) of the Securities Act, the name of the intermediary through which the offering is being conducted, and a link directing the potential investor to the intermediary's platform;

(b) the terms of the offering, which means the amount of securities offered, the nature of the securities, the price of the securities, and the closing date of the offering period; and

(c) factual information about the legal identity and business location of the issuer, limited to the name of the issuer of the security, the address, phone number, and website of the issuer, the e-mail address of a representative of the issuer, and a brief description of the business of the issuer.

Although advertising the terms of the offering off of the intermediary's platform is limited to a brief notice, an issuer may communicate with investors and potential investors about the terms of the offering through communication channels provided on the intermediary's platform. An issuer must identify itself as the issuer and persons acting on behalf of the issuer must identify their affiliation with the issuer in all communications on the intermediary's platform.

An issuer is allowed to compensate others to promote its crowdfunding offerings through communication channels provided by an intermediary, but only if the issuer takes reasonable steps to ensure that the promoter clearly discloses the compensation with each communication.

5. Restrictions on Resale

Securities purchased in a crowdfunding transaction generally cannot be resold for a period of one year, unless the securities are transferred:

(1) to the issuer of the securities;

(2) to an "accredited investor";

(3) as part of an offering registered with the Commission; or

(4) to a member of the family of the purchaser or the equivalent, to a trust controlled by the purchaser, to a trust created for the benefit of a member of the family of the purchaser or the equivalent, or in connection with the death or divorce of the purchaser or other similar circumstance.

6. Exemption from Section 12(g)

Section 12(g) of the Exchange Act requires an issuer with total assets of more than \$10 million and a class of securities held of record by either 2,000 persons, or 500 persons who are not accredited investors, to register that class of securities with the Commission. However, securities issued pursuant to Regulation Crowdfunding are conditionally exempted from the record holder count under Section 12(g) if the following conditions are met:

- the issuer is current in its ongoing annual reports required pursuant to Regulation Crowdfunding;
- has total assets as of the end of its last fiscal year of \$25 million or less; and
- has engaged the services of a transfer agent registered with the SEC.

As a result, Section 12(g) registration is required if an issuer has, on the last day of its

fiscal year, total assets greater than \$25 million and the class of equity securities is held by more than 2,000 persons, or 500 persons who are not accredited investors. In that circumstance, an issuer is granted a two-year transition period before it is required to register its class of securities pursuant to Section 12(g), so long as it timely files all of the annual reports required by Regulation Crowdfunding during such period.

An issuer seeking to exclude a person from the record holder count of Section 12(g) is responsible for demonstrating that the securities held by the person were initially issued in an offering made under Section 4(a)(6).

7. Bad Actor Disqualification

Rule 503 of Regulation Crowdfunding includes “bad actor” disqualification provisions that disqualify offerings if the issuer or other “covered persons” have experienced a disqualifying event, such as being convicted of, or subject to court or administrative sanctions for, securities fraud or other violations of specified laws.

a. Covered Persons

Understanding the categories of persons that are covered by Rule 503 is important because issuers are required to conduct a factual inquiry to determine whether any covered person has had a disqualifying event, and the existence of such an event will generally disqualify the offering from reliance on Regulation Crowdfunding.

“Covered persons” include:

- the issuer, including its predecessors and affiliated issuers;
- directors, officers, general partners or managing members of the issuer;
- beneficial owners of 20% or more of the issuer’s outstanding voting equity securities, calculated on the basis of voting power;
- promoters connected with the issuer in any capacity at time of sale; and
- persons compensated for soliciting investors, including the general partners, directors, officers or managing members of any such solicitor.

b. Disqualifying Events

Under the final rule, disqualifying events include:

- Certain criminal convictions;
- Certain court injunctions and restraining orders;
- Certain final orders of certain state and federal regulators;
- Certain SEC disciplinary orders;
- Certain SEC cease-and-desist orders;
- Suspension or expulsion from membership in a self-regulatory organization (SRO), such as FINRA, or being barred from association with an SRO member;
- SEC stop orders and orders suspending the Regulation A exemption; and
- U.S. Postal Service false representation orders.

Many disqualifying events include a look-back period (for example, a court injunction that was issued within the last five years or a regulatory order that was issued within the last ten years). The look-back period is measured from the date of the disqualifying event – for example, the issuance of the injunction or regulatory order and not the date of the underlying conduct that led to the disqualifying event – to the date of the filing of an offering statement.

Disqualification will not arise as a result of disqualifying events relating to any conviction, order, judgment, decree, suspension, expulsion or bar that occurred before May 16, 2016, the effective date of Regulation Crowdfunding. Matters that existed before the effective date of Regulation Crowdfunding, are still within the relevant look-back period, and would otherwise be disqualifying are, however, required to be disclosed in the issuer’s offering statement.

c. Exceptions and Waivers

Regulation Crowdfunding provides an exception from disqualification when the issuer is able to demonstrate that it did not know and, in the exercise of reasonable care, could not have known that a covered person with a disqualifying event participated in the offering.

The steps an issuer should take to exercise reasonable care will vary according to particular facts and circumstances. An instruction to the rule states that an issuer will not be able to establish that it has exercised reasonable care unless it has made, in light of the circumstances, factual inquiry into whether any disqualifications exist.

Disqualification will not arise if, before the filing of the offering statement, the court or regulatory authority that entered the relevant order, judgment or decree advises in writing – whether in the relevant judgment, order or decree or separately to the Commission or its staff – that disqualification under Regulation Crowdfunding should not arise as a consequence of such order, judgment or decree.

Regulation Crowdfunding also provides for the ability to seek waivers from disqualification by the Commission upon a showing of good cause that it is not necessary under the circumstances that the exemption be denied.

8. Other Resources

The adopting release Regulation Crowdfunding can be found on the SEC's website at <http://www.sec.gov/rules/final/2015/33-9974.pdf>.

Regulation Crowdfunding (17 CFR 227.100 et seq.) can be accessed through the "Corporation Finance" section of the SEC's website at <http://www.sec.gov/divisions/corpfin/ecfrlinks.shtml>.

You can also submit complaints or tips about possible securities laws violations on the SEC's questions and complaints page at <http://www.sec.gov/complaint.shtml>.

9. Contacting the SEC Staff

The SEC staff is happy to assist with questions regarding Regulation Crowdfunding. For issuer questions, you may contact the Division of Corporation Finance's Office of Small Business Policy using this [online request form](#) at or by telephone at (202) 551-3460. For intermediary questions, you may contact the Division of Trading and Markets, Office of Chief Counsel, at (202) 551-5777, or search for your answer in the [Small Business Compliance Guide for Intermediaries](#).

[1] This guide was prepared by the staff of the U.S. Securities and Exchange Commission (the "Commission") as a "small entity compliance guide" under Section 212 of the Small Business Regulatory Enforcement Fairness Act of 1996, as amended. The guide summarizes and explains the rules adopted by the SEC, but is not a substitute for any rule itself. Only the rule itself can provide complete and definitive information regarding its requirements.

[2] Crowdfunding is a relatively new and evolving method of using the Internet to raise capital to support a wide range of ideas and ventures. An entity or individual raising funds through crowdfunding typically seeks small individual contributions from a large number of people. Individuals interested in the crowdfunding campaign – members of the "crowd" – may share information about the project, cause, idea or business with each other and use the information to decide whether to fund the campaign based on the collective "wisdom of the crowd."

[3] The Regulation Crowdfunding adopting release is available at <http://www.sec.gov/rules/final/2015/33-9974.pdf>. The staff has also issued a small entity compliance guide concerning registration of funding portals, which is available at <http://www.sec.gov/divisions/marketreg/tmcompliance/fpregistrationguide.htm>.

[4] This "Investment Limit" column reflects the aggregate investment limit across all Regulation Crowdfunding offerings within a 12-month period.

Modified: July 5, 2016

ISA Boutique is utilizing the hybrid solution to identify which products are of interest to shoppers, as well as where inventory is located and when it requires replenishment.

By Claire Swedberg

Tags: Retail, Inventory / Warehouse Management

Mar 18, 2016—ISA Fashion Boutique International Ltd., a seller of international luxury brands in Hong Kong, mainland China and Macau, has deployed an RFID-based inventory-management system provided by Hong Kong IT services company [PCCW Solutions](#). The system enables the retailer to track the locations of products, engage with customers, learn their preferences and reduce labor costs based on inventory counts. The solution, known as Inifinitum Retail, includes IP cameras as well as ultrahigh-frequency (UHF) RFID readers. As a result of the improved inventory management, the retailer says that it plans to deploy the system this year at all 11 of its stores. [Alpha Solution Ltd.](#) installed the technology.

Traditionally, RFID has had limitations since it can track a tagged product, but not necessarily link that item with a particular customer, explains Jacky Ting, PCCW Solutions' digital practice leader. By itself, RFID cannot enable a store to forward product information and promotions to shoppers. However, by linking RFID data to closed-circuit television (CCTV) camera images and social-media sites such as [Facebook](#), a retailer can identify where shopper traffic is heaviest (using a camera-based heat map), understand how an individual responds to a product (by tracking the expressions on his or her face) and monitor comments that its customers make on social media (with their permission), using the store's Wi-Fi network.



The reader built into an ISA store's EAS gate can capture the ID number of a customer's RFID-enabled loyalty card, prompting the Inifinitum Retail software to send promotional offers to that individual's phone, based on his or her previous purchasing behavior.

Inifinitum Retail aims to overcome a variety of problems that stores face, says Wing Lee, PCCW Solutions' senior VP, such as understanding which products interest customers, and then approaching them with relevant offers. ISA Boutique uses camera images only for tracking shoppers' locations within its stores, Lee notes, while it could opt to use facial analytics in the future to

identify each customer's age, race, gender and response to products based on facial expressions.

In 2012, ISA Fashion first installed an RFID system for counting inventory and tracking product locations at one of its stores with the help of Alpha Solution (see [ISA Boutique Tracks Inventory, Shopper Behavior Via RFID](#)). The system, which is still in use, employs tiny RFID labels attached to jewelry, as well as readers installed in display cabinets, to track when goods are on display and when they are removed from a cabinet. After Infinitem Retail was released in October 2015, the retailer began using the system to track all of its products, which also include clothing, leather goods, eyewear and watches, at three shops and one warehouse in Hong Kong, as well as a single shop in mainland China. The new solution includes the use of electronic article surveillance (EAS) hard tags for non-jewelry products.

Infinitem Retail consists of RFID readers built into the EAS gate at the door, as well as a feature known as iR-Furniture—RFID interrogators built into shelves to read tags in real time. The system also includes readers installed at checkout terminals. In the warehouse, readers are used to identify when goods are received and then shipped to a store.

At the warehouse, an EAS hard tag with a built-in EPC Gen 2 ultrahigh-frequency (UHF) RFID inlay is attached to each product other than jewelry. The inlay is read at the warehouse for inventory purposes, and the cloud-based hosted software is automatically updated to indicate, for instance, if a tagged item has been shipped, as well as to which store and when this occurred.

Upon arrival at the store, some goods are placed on iR-Furniture shelves, where they are then tracked in real time. Those items consist of products other than the small jewelry that is monitored via the jewelry-tracking cabinets which the retailer first deployed last year. In the sections of the store in which iR-Furniture is used, readers capture tag ID numbers until an item is removed from the display. The software identifies that action and can issue an alert if the item is not returned to that location or purchased, says Tafe Tsai, Alpha Solution's director.

Additionally, after a store closes at the end of the business day, employees can log into the software to determine whether all products are on the iR-Furniture shelving, instead of having to check every item one at a time.



Jacky Ting, PCCW Solutions' digital practice leader

Customers also carry RFID-enabled loyalty cards so that they can be recognized as they arrive at the store. This enables them to receive offers on their smartphone, based on their location within the building.

The reader built into the EAS gate can capture the ID number of each customer's loyalty card and forward that data to the hosted software, which identifies that shopper's buying habits based on a record of coupons redeemed and purchases made by that individual. The software forwards offers and coupons to that individual's phone, based on his or her previous purchasing behavior.

When a customer brings a tagged product to the cash register at the point of sale, a counter-top RFID reader captures the ID number of that item's RFID tag, links it to the product's stock-keeping unit (SKU) and removes that item from the inventory list. An employee then detaches the hard tag from the object. In that way, as the individual walks out of the store with his or her purchases, the EAS gate is not alerted. That data enables the store to replenish a product as soon as it is purchased or taken off the premises.

CCTV cameras are used to identify where shoppers travel within the store, and where they spend the most time. The software can then compare that information with sales data in order to determine which items are attracting attention, as well as whether they are being purchased.

Because shoppers often interact on their phone while making a purchasing decision, the store also wanted to be able to know what was being said about their products online. Therefore, customers can use the store's Wi-Fi network, but must first provide their social network ID so that the retailer can view comments about its products between shoppers and their friends. Once a customer attempts to connect with the in-store's Wi-Fi access point, a Web link pops up on that person's devices, asking him or her to connect with the retailers' social-media platforms, such as Facebook, [Twitter](#) or [WeChat](#). The shopper is then directed to the corresponding social-media application. Once customers "like" or "follow" the retailer's social-media platforms, they can then use the in-store Wi-Fi.

Adopting Infitum Retail enables ISA Boutique to have a deeper understanding of customers' demographic and behavior, Tsai explains. The data analytics provides the retailer with the information it needs to design effective marketing campaigns, he adds.



Wing Lee, PCCW Solutions' senior VP

According to Lee, ISA has reported that its use of Infitum Retail has led to an increase in sales amount and volume, while reducing costs due to the decreased workforce required to track inventory. Since the system was taken live at ISA Boutique, he says, the retailer has reported increased operational efficiency and sales, as well as decreased expenditures thanks to a reduction in human resources.

Infitum Retail also has a facial-analytics component, though ISA Boutique is not yet using this feature. With the system, the CCTV camera captures an image of a person's face and passes that photo to the Infitum Retail software's video-analytical algorithm so that it can estimate demographic information, such as gender, race, age range and expression (such as smiling). "For the sake of accurate analytical result," Lee states, "the CCTV or camera should be located in the area of sufficient lighting and [be] able to capture the front side of the whole faces of customers." That information would help the retailer to understand what kinds of customers are interested in a product, he explains, and to ascertain their level of interest based on their facial expressions.

IR-Furniture read data can be paired with this facial-analytics data to identify which items customers pick up. Infitum Retail has been launched since early October 2015, Lee says, and ISA Boutique is among its first customers.

"In the IoT era," Ting says, "our major focus should be placed on the utilization of solution and information under the customer-centric business environment." He adds that "understanding customers' behavior and needs can help retailers with the market share."

Why Luxury Brands Are Putting Microchips in Your Clothes and Accessories

The same technology powering payments on your iPhone is now being used to identify knockoff designer goods.

[Lauren Indvik](#)

Apr 14, 2016



A woman overlooks a shop on New York's famed Canal Street. Photo: Spencer Platt/Getty Images

Fakes are everywhere. The flash of an "LV" logo on New York's busy Canal Street, or a pile of lookalike Chanel bags at Istanbul's Grand Bazaar, hardly warrants a raised eyebrow these days. But counterfeiting continues to plague the luxury sector, costing European clothing and accessories companies an [estimated](#) €26.3 billion (\$30 billion) — about 10 percent of their sales — every year, and doing damage to the reputation of their brands to boot. Those of us who've ever been duped into buying a replica Hermès scarf at a secondhand store, or a knockoff Marc Jacobs bag on Ebay, have felt the pain of counterfeiting all too well.



Moncler is now including RFID tags in all of its goods, allowing customers to verify the authenticity of their purchases. Photo: Moncler

Brands have long turned to trade associations and law enforcement agencies in costly efforts to shut down those making and selling knockoffs, but recently, they've also begun to seek out more technologically driven solutions. Last week, [Moncler](#) announced that beginning with its spring/summer 2016 collection, all of its products will contain small radio frequency identification (RFID) chips, each containing a unique ID that will allow users to scan and authenticate their goods via their smartphones or through the [code.moncler.com](#) website. Employing the same technology that allows Apple Pay users to swipe their phones at cash registers in lieu of pulling out their credit cards, it will make it far easier for customers to identify if the \$1,200, Moncler-branded down coat they've just bought is a fake — no [online guide](#) necessary. (Counterfeits are so rampant, in fact, that Moncler has a whole team in its customer service department dedicated to supporting clients who have purchased them.)

Moncler isn't the only Italian-based luxury brand to use microchips in the battle against counterfeiting. Beginning with its pre-fall 2014 collection, [Salvatore Ferragamo](#) began embedding RFID chips into the left soles of its women's shoes to allow the company to verify their authenticity. It has since added the tags to products in other categories, including women's bags and luggage and men's shoes and small leather goods.

RFID chips are not new — even in the retail sphere. Major merchants including Walmart and the UK's Marks & Spencer chain have for years been working with their suppliers to attach RFID tags to products in order to help with inventory tracking and management, allowing those retailers to quickly assess where products are in the supply chain; how many they have in stock at a given warehouse, store or even specific clothing rack; and replenish accordingly. (Moncler also uses its chips for inventory purposes, a spokesperson tells *Fashionista*.) Brands like the accessibly priced German women's clothier [Gerry Weber](#), which added RFID chips to its care tags in 2011, have seen double-digit sales increases almost immediately after integrating the technology, simply because they are able to restock their products more accurately and efficiently, says Steven Owen, executive vice president of sales and marketing at [NXP Semiconductors](#), which makes Gerry Weber's tags as well as those for Pfizer's Viagra brand. Other companies have used it to fight theft, using the unique serial numbers in the RFID chips to prevent people from returning unregistered (i.e., stolen) products to stores, or to target suppliers illegally producing excess stock and selling them on the open market.

So why are luxury brands getting involved now? Owen says that though there's been a clear business case for years, companies have been slow to adopt the technology, in part because building a system that identifies and tracks a company's entire catalog requires a considerable investment, costing a "couple of million dollars" for a small to medium-sized company to start. The proposition has also become more attractive as the quality and sophistication of

these systems has improved, and as the size and price of chips have gone down. It costs Gerry Weber, for example, 9 cents to tag each of the approximately 30 million garments it produces each year.

As with any new technology — particularly of the tracking variety — [privacy concerns abound](#). Gerry Weber deactivates its chips at point-of-sale, but for Moncler and Ferragamo, that would defeat the purpose. In Europe, where data privacy laws are more strict, "you have to tell the client if you're providing such a product with an RFID chip and serial number," says Owen. Indeed, Burberry discloses its uses of RFID [on its website](#). There are [some U.S. state laws](#) prohibiting, for example, the surreptitious scanning of RFID chips in ID cards, but nothing requiring that a retailer disclose chips are embedded in the products they sell.

It's not hard to imagine a day in which everything — from our razors to the dollar bills in our wallets — are embedded with microchips. And the technology will only get more sophisticated over time. Last year, for example, researchers at Nottingham Trent University in the UK [unveiled a prototype](#) for embedding RFID chips into yarns. Three months ago, they launched a company, Advanced E-Textiles Ltd, to bring it to market.

BURBERRY PRIVACY POLICY: RFID

Since September 2012, we have started to implement the use of Radio Frequency Identification ("RFID") technology within some of our flagship stores.

What is RFID Technology?

RFID technology provides us with a way of identifying individual product items using radio signals. RFID technology is found in a small tag typically in the swing ticket but in some cases is embedded in the product via a textile RFID label. By using RFID wireless readers at various points in our stock control process and in selected stores, we can read information about our products, such as the product type and range within an RFID wireless reader area.

Why is Burberry using RFID technology?

We have started to initiate the use of RFID technology throughout our Burberry product lines to assist with stock and quality control, while also enhancing the customer experience in selected stores. RFID technology enables customers to view bespoke multimedia content specific to different products and ranges on in-store display screens.

The RFID tags do not, on their own, carry or store any personal data which could identify individual customers to us. We only store product specific information such as the product code on the RFID tag. This information is not linked to a customer, or to customer transactions. It is possible that in the future we may link the RFID tags to our customer database, however we will not do this unless we have the prior consent of our customers to do so.

Can I de-activate or remove the RFID tags from my purchased items?

Yes. Within selected stores, our Sales Associates will assist you if you wish to have the RFID tags within your purchases de-activated for the triggering of bespoke multimedia content. We will not de-activate the RFID element which relates to stock and quality control.

If you are buying products online or would like to deactivate the interactive multimedia element at a later date, you can do so by simply removing the textile RFID label. If you require help with this, please contact [Customer Service](#) who will be able to assist. Any information which is stored on the RFID tags will not be stored for any longer than is necessary.

Are there any environmental concerns?

There are clear European rules in place for data transmission through radio signals and our RFID tags comply with these rules and guidance. Frequencies within our RFID tags have been selected

to ensure that, as far as possible and when considering current scientific findings, no known health risks can occur when using this technology.



Privacy trade-offs in retail tracking

Ashkan Soltani, Chief Technologist

Apr 30, 2015

TAGS: [MAC address tracking](#) | [Mobile device settings](#) | [Mobile location analytics](#)

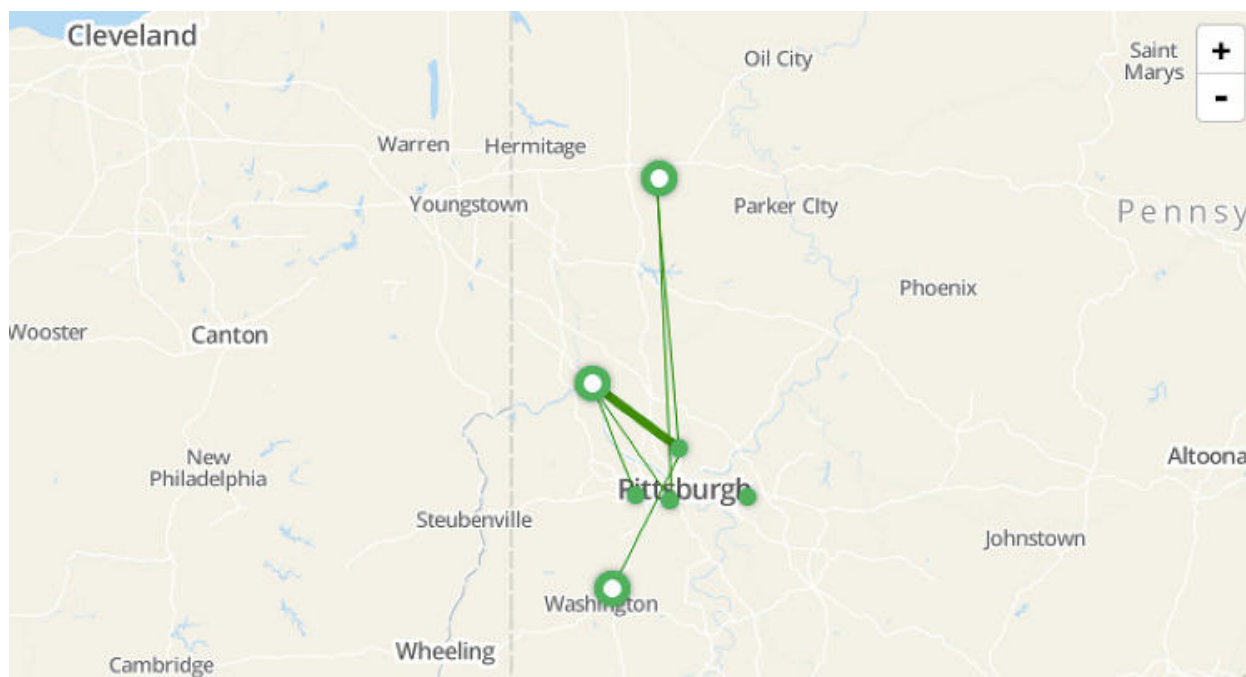


Figure 1 Identifying customers that visit multiple retail locations for the same store
 (Source: Fast Company, "[Here's What Brick-And-Mortar Stores See When They Track You](#)")

Last week, the [FTC](#) announced a proposed settlement with [Nomi Technologies](#), a retail tracking firm that monitors consumers' movements through stores, for failing to adhere to their opt-out promises.

Nomi's Listen Service tracks consumers by monitoring the location of their devices as they move about. The approach does not identify an individual by name but instead monitors unique wireless identifiers emitted by the smartphones, wearables, and other wireless accessories that consumers carry.

The obscure nature of retail tracking technology has been somewhat controversial. On a number of occasions, retailers such as [Nordstrom](#) and [Philz Coffee](#), and cities, such as the [City of London](#), have discontinued its use once their consumers were made aware of the practice and expressed privacy concerns.

For context of consumer concern over this practice, a recent [OpinionLab](#) survey of 1,000 consumers indicated that, "8 out of 10 shoppers do not want stores to track their movements via smartphone" and "nearly half (43%) of shoppers are less likely to shop at a favorite retailer if the brand implements a tracking program."

The privacy issues are further exacerbated by the fact that most consumers are not aware that their device information

may be captured as they walk by a store or visit an airport.

In light of the Commission's proposed settlement with Nomi and the ongoing public debate, I thought it would be worthwhile to describe how different retail tracking technologies work, and in my opinion, the specific privacy trade-offs of each approach. My predecessor, Latanya Sweeney, has also [blogged](#) about this topic and the FTC held a [seminar](#) last spring, where I presented an overview on how some of this technology works.

OVERVIEW

Retail tracking generally works by monitoring individual's movements in or near locations of interest. The specific mechanisms can vary but often involve recording signals emanated by the individual or their devices as they move about.

For example, early retail analytics services relied on in-store cameras to optically record individual's movements (reflected "photon emanations" to be geeky) in order to count foot traffic or create heat maps of which product displays might be most popular. This technique was also a topic of discussion at an [FTC workshop on facial recognition](#). Video retail analytics, while providing rich in-store patterns, typically does not employ facial recognition and therefore provides a somewhat higher degree of "practical obscurity" since it cannot identify consumers or link them across locations.

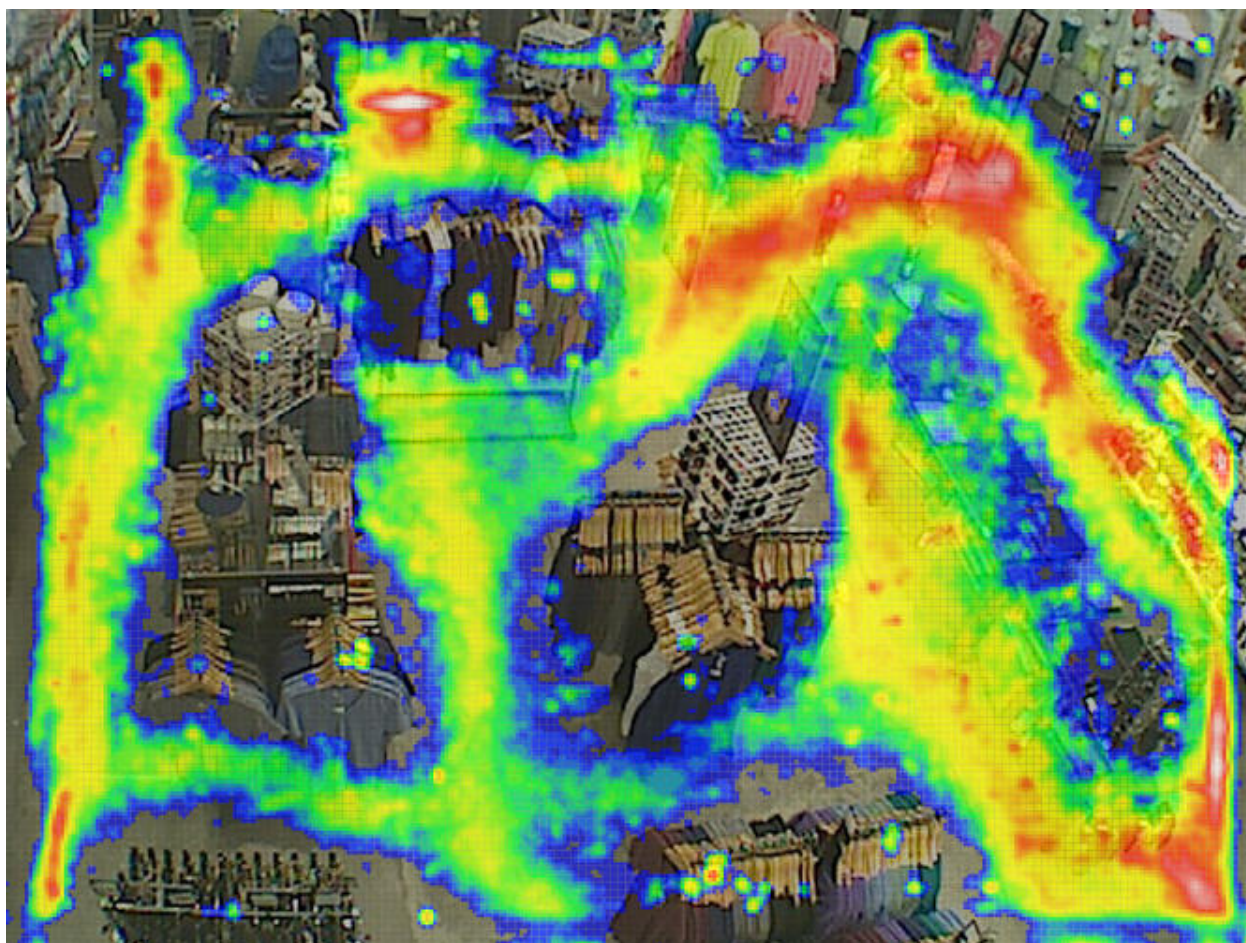


Figure 2 Example heatmap from a video based retail location system.
(Source: [Here's What Brick-And-Mortar Stores See When They Track You](#))

Newer approaches monitor signals broadcast from individual's devices as the device *searches for* or *communicates with* nearby devices and networks. This can consist of "*active monitoring*," which is typically performed by the service the device is communicating with, such as by the cellular provider or by the WiFi hotspot the device is connected to. The other approach is '*passive monitoring*', which intercepts signals from the device as it communicates or searches for **other** devices and networks.

For example, some passive retail analytics techniques intercept your communication to the cellular provider, or the beacons broadcast by your device as it searches for nearby WiFi hotspots. Most modern cellphones and wearables have an array of wireless antennas that regularly broadcast signals as they search for or communicate with cellular, WiFi, and Bluetooth networks – even when they are not in use. Note, the information collected is often referred to as “signaling information” in the header of the communication and distinguished from the actual contents which are typically not collected as this could potentially run afoul of wiretapping laws. It's also worth noting that other signals, including “Near Field Communication” (NFC), LED, and even acoustic signals, are used by retail analytics firms use to track individuals. However, I will limit the discussion to the most prominent.

By monitoring the strength of these signals and the associated identifier, the retailer is able to ascertain the volume of visitors to their store, the frequency with which visitors return, the behavior of passers-by, or even the demographics of visitors to a particular location (as in the case of carrier-provided retail analytics).

The privacy concerns will ultimately be impacted by the identifier used (i.e., how persistent it is or the effectiveness of obfuscation), consumer awareness (or notice), and availability of choice or “opt-out” mechanisms, which I lay out below.

IDENTIFIERS

Retail analytics firms track these signals and associated identifier(s) in order to triangulate and record the location of an individual device. As such, the identifiers themselves can vary and present different privacy concerns.

Active monitoring by your cellular carrier is often based on persistent identifiers associated to your mobile devices – which can include your International Mobile Station Equipment Identity (IMEI), International Mobile Subscriber Identity (IMSI), or Mobile Station ISDN (MSISDN), which is assigned when you purchase your device and SIM card. The carrier relies on these numbers to provide service and can also use them to generate aggregate analytics to retailers.

In contrast, passive cellular tracking techniques utilizes Temporary Mobile Subscriber Identifiers (TMSI) that are assigned by the carrier but rotate over the course of period of hours to weeks, depending on the configuration of the cellular network. Use of this identifier inherently provides some privacy protections over hardware identifiers since the rotating identifier limits the amount of time an individual's behavior can be linked. For example, repeat visits over the course of the week can be tied back to the same individual, but not over the course of a month or a year. Technology to passively track persistent cellular identifiers such as IMSI is also readily available (known as “IMSI catchers”), however, to my knowledge, its use has primarily been limited to law enforcement uses.

Similarly, hardware identifiers such as WiFi or Bluetooth Media Access Control (MAC) addresses are persistent throughout the life of the device since they are tied to the physical embedded chipsets. As part of the wireless protocol(s), these identifiers are automatically broadcast when devices search for networks or communicate with other devices, including wireless access points, wireless headsets, and health trackers -- so they are visible to a broader set of observers.

This persistent identifiers often can be linked to individuals by name. For example, when you sign into a commercial WiFi hotspot, your MAC address is tied to the information you use to sign up for the service. Additionally, automatic WiFi probes also broadcast the names of last networks a device has connected to, which potentially reveal additional information about the individual, such as the name of their home or work network (i.e., “FTC Wireless”). This information could allow observers to link a MAC address to a given user or network, but it is unclear whether any companies collect or use this information.

Finally, in the case of smartphones, apps and advertisers sometimes rely on MAC addresses as a mechanism to uniquely track behavior online -- thereby providing a mechanism for linking offline (physical) and online behavior.

As a result of sensitivities associated with hardware identifiers, some smartphone manufacturers have attempted to build in features which limit retail tracking by randomizing the device's wireless identifier (MAC address) when the device is not in use, although its effectiveness is somewhat limited. The Internet Engineering Task Force (an internet standards body) is also experimenting with ways to improve smartphone privacy by randomizing MAC address.

Some retail analytics providers, including Nomi, cryptographically hash the identifier prior to retention in an attempt to reduce some of the privacy concerns. This “hashing” attempts to obfuscate the original identifier (such as MAC address) while still providing a unique string which can be used to identify the device over time and space. As stated in the FTC’s complaint:

“Nomi cryptographically hashes the MAC addresses it observes prior to storing them on its servers. Hashing obfuscates the MAC address, but the result is still a persistent unique identifier for that mobile device. Each time a MAC address is run through the same hash function, the resulting identifier will be the same. For example, if MAC address 1A:2B:3C:4D:5E:6F is run through Nomi’s hash function on ten different occasions, the resulting identifier will be the same each time. As a result, while Nomi does not store the MAC address, it does store a persistent unique identifier for each mobile device. Nomi collected information about approximately nine million unique mobile devices between January 2013 and September 2013.”

However, hashing is also of limited effectiveness as described in the majority statement:

“Although Nomi took steps to obscure the MAC addresses it collected by cryptographically hashing them, hashing generates a unique number that can be used to identify a device throughout its lifetime and is a process that can easily be “reversed” to reveal the original MAC address. See, e.g., Jonathan Mayer, Questionable Crypto in Retail Analytics, March 19, 2014, <http://webpolicy.org/2014/03/19/questionable-crypto-in-retail-analytics/> (describing successful efforts in “reversing the hash” to identify the original MAC address).”

Essentially, while hashing attempts to remove some of the risk associated with use of a persistent hardware identifier, it is often easy to circumvent. In fact, free precomputed tables of known hashes (rainbow tables) are available that make reversing known hashes practically instantaneous.

In addition, even hashed, the use of a persistent identifier presents privacy issues since tracking pattern of movement in itself is often enough to uniquely identify an individual. As this technology becomes more widespread, a single retail analytics firm that services multiple retail chains will be able to collect a large pattern of individual’s movements, even if the information is not shared between unaffiliated chains.

NOTICE

These various approaches also vary to the degree of notice that is offered to consumers.

For the active forms of tracking, consumers are typically given notice when first signing up to the service, such as in the case of purchasing cellular service or logging into a commercial WiFi hotspot. In the case of iBeacons, consumers typically enable a feature on their phone or download an app which does the “tracking.” (Note: in the case of active Bluetooth monitoring via iBeacons, it’s actually the consumer’s phone that “tracks” the retail location and sends information back to the retail provider.)

However, many of the non-active techniques passively record signals so there’s technically no way to detect and be made aware of the activity without signage to that effect. One industry self-regulatory group’s code of conduct requires retail analytics firms to “take reasonable steps to require that companies using their technology display, in a conspicuous location, signage that informs consumers about the collection and use of MLA Data at that location.” However, not all retail analytics companies adhere to these principles, nor do any of the retailers that would be responsible for implementing in-store signage, making the notice essentially voluntary.

Finally, wireless signals are typically not constrained by store walls so visitors driving by or visiting a neighboring store will likely not be aware of the presence of retail location tracking in neighboring stores. Similarly, signage will have similar limitations for retail location techniques utilizing drones.

CHOICE

Some of the retail analytics techniques are opt-in, such as iBeacon and location enabled shopping apps. However, the

passive techniques typically operate under an opt-out regime, as do the carrier-based methods.

Once consumers are made aware, some of the firms allow the consumers to opt-out. For example, [AT&T](#) and [Verizon](#) provide dashboards by which consumers can manage their privacy preferences and opt out of having their location information used for marketing purposes.

Mobile analytics companies that rely on passive WiFi tracking technologies and adhere to the smart-places principles allow users to opt out by entering their MAC address into the [Smart Places opt-out form](#). However, the principles do not allow individuals to opt-out from data collection for the purpose of network management or security.

With the exception of turning off their devices or putting them into “airplane” mode, there is currently no way to avoid collection altogether since opt-out processing typically occurs during retention. That is, sensors or carriers still collect consumer’s activities at the point of interest, then process the opt-out before being stored on their backend systems.

Personal health trackers and other wearables typically do not have an easy way to identify their MAC address and some do not have “Off” buttons, which constrains consumers’ ability to limit tracking of these devices.

ANALYSIS

	IDENTIFIER	NOTICE	CHOICE
In-store Camera	None [1]	Signage optional	None
Active Cellular	Persistent (IMEI/IMSI/MSISDN)	Typically provided during Carrier Signup	opt-out via carrier
Passive Cellular	Temporary (TMSI [2])	Signage optional [3]	None
Active WiFi	Persistent (WiFi MAC)	Typically provided during WiFi sign-up	NA / opt-in (based on hotspot terms)
Passive WiFi	Persistent (WiFi MAC)	Signage optional [3]	Smart-places.org for participating MLAs [4]
Active Bluetooth	Varies based on app and OS features	Notice provided during app install	opt-in
Passive Bluetooth	Persistent (BT MAC)	Signage optional [3]	Smart-places.org for participating MLAs [4]
	1 - This excludes facial recognition, which at the present time is not in use for retail tracking		
	2 - Based on statements from Path Intelligence CEO, a MLA- utilizing passive cellular		
	3 - Mobile analytics providers must “take steps” -- but not strictly required. Neighboring stores and		

	sidewalks limited.
	4 - Opt-out for wearables and other accessories limited

Retail tracking has many benefits for retailers and consumers alike. Stores are able to better understand the behaviors and preferences of their shoppers, and individuals are in turn, receive better service. However, the technology does present privacy trade-offs.

I've attempted to highlight some of the trade-offs of the various mobile retail tracking techniques. Given the variety of approaches, there are a number of things that industry could do to alleviate the privacy concerns and address some of the gaps in consumer awareness.

For example, at the FTC's 2013 seminar on mobile device tracking, I suggested that passive retail analytics technology devices could automatically broadcast standardized, semi-continuous wireless signals that announce their presence as a technical solution to pervasive computing in the public sphere. One could imagine open WiFi or Bluetooth networks which alert users to the existence of mobile retail tracking and allow them to temporarily join in order to opt-out. Additionally, industry or individuals could develop privacy enhancing apps that allow privacy conscious users to automatically disable transmission of signals when approaching these networks in order to avoid collection altogether.

There are also additional technical measures that could provide additional privacy protections for identifiers, such as hashing the incoming identifiers **at the time of capture** with rotating salts based on time or retail location. This would provide protections similar to the TMSI, which prevents linking activity to the same device over long periods of time or across multiple locations (in the case of the location-based salt).

These are just some of the potential ways to evaluate and address the trade-offs with this emerging technology.

The author's views are his or her own, and do not necessarily represent the views of the Commission or any Commissioner.



ftc.gov

LANDSLIDE[®]

A PUBLICATION OF THE ABA SECTION OF INTELLECTUAL PROPERTY LAW

IoT Big Data: Consumer Wearables, Data Privacy and Security

Vol. 8 No. 2

By Katherine Britton

Katherine E. Britton has her own practice, is of counsel at Simmons Legal, PLLC, and is an affiliate professor at the University of North Texas Dallas College of Law in Dallas, Texas. Katherine specializes in complex civil litigation, employment and human resources counseling, probate, estate planning, consumer protection, and privacy law matters. Katherine is a Certified Information Privacy Professional (CIPP/US) through the International Association of Privacy Professionals and is admitted to the bars in Illinois, the District of Columbia, and Texas.

[T]he world contains an unimaginably vast amount of digital information which is getting ever vaster ever more rapidly. . . . The effect is being felt everywhere, from business to science, from government to the arts. Scientists and computer engineers have coined a new term for the phenomenon: "big data."¹

In the United States, the age of big data is upon us. In 1965, Intel co-founder Gordon Moore predicted that the number of transistors on a computer chip would double every two years while the chip's price would remain constant. "Moore's law" meant consumers could buy the same technology two years later for about the same

price. Fifty years later, Moore's prediction has remained remarkably accurate to the point that technology companies have recognized Moore's law as a benchmark they must meet, or fall behind in the market.² The wearables market generally follows Moore's law, creating a "mad rush" among companies to bring products to market. Consumers have come to expect technological products to be faster, cheaper, and more compact over time; this expectation has driven trends of rapid growth in computing power, smaller devices, better battery life, ability to connect to the Internet, and reduction in cost.

Ideally, this consumer demand should drive the market; however, the wearables market poses certain intellectual property imperfections pertaining to data privacy. For example, consumers have imperfect information about how companies collect and use personal data. Federal data privacy regulations in the United States focus on following the Fair Information Practice Principles: notice, choice, access, accuracy, data minimization, security, and accountability. Third-hand collected personal data—the data of consumers who do not use wearables but whose data are collected by others' wearables—would not be protected by the Fair Information Practice Principles.

The benefits wearables pose to consumers are considerable, assuming data security and data privacy concerns are addressed. This article explores the existing and developing infrastructure and technological features supporting wearables, the specific data privacy and security concerns wearables pose in the United States commercial sphere in the age of big data, particularly in the healthcare space, and the idea that policymakers should address the data privacy and security concerns posed by wearables because consumers and businesses are unlikely to do so.

IoT Infrastructure Supporting Wearables Might Not Address Data Privacy or Security

IoT Connectivity Is Based on RFID Technologies

Kevin Ashton, one of the founders of the Massachusetts Institute of Technology (MIT) Auto-ID Center, is credited with coining the term "the Internet of Things" (IoT). The term refers to objects embedded with technologies like microchips, sensors, and actuators that often use Internet Protocol (IP) and share data with other machines or software over communications networks. Wearable computing devices, or "wearables," are a subset of IoT. The MIT Auto-ID Center was founded in 1999 with the mission of pioneering a global open standard system for radio-frequency identification (RFID) technologies. By developing RFID technologies, the Center laid the foundation for the many architectures supporting IoT.

RFID technologies use radio waves, microchips, and antennas to identify people, products, and objects automatically. RFID technologies use machine-to-machine (M2M) transmissions, which refer to direct communications between machines such as a microchip and a microchip scanner, a wearable and a third-party application (app), or a wearable and a monitoring hub. M2M transmissions share information without any special configuration or other setup requirements. For example, veterinarians use RFID technology to identify missing microchipped pets. In 2004, the Food and Drug Administration (FDA) approved a similar technology for use on humans.³ The technology relies on a slender capsule of bioglass imbedded in the skin. That capsule contains a microchip with a unique serial number, and is attached to a tiny antenna (the chip and the antenna together are called an RFID transponder or an RFID tag). The capsule's sole function is to store and transmit a unique identification code to a reader. The code can be read with a microchip scanner passed over the skin. The reader converts the radio waves reflected back from the RFID tag into digital information that can be compared to a veterinary or medical database.

IoT Connectivity Relies on Systems That Handle Security Independently

Wearables are subject to cybersecurity attacks. In April 2014, a vulnerability in Internet encryption (named the Heartbleed bug) was so widespread that it affected wearables.⁴ The Federal Trade Commission (FTC) held a workshop titled "Internet of Things: Privacy and Security in a Connected World" (FTC Workshop), solicited public comments, and published a staff report in January 2015 summarizing the various viewpoints. When considering how to handle data security, there was widespread agreement among panelists at the FTC Workshop on the need for companies manufacturing IoT devices to incorporate reasonable security measures.⁵ These devices, however, also rely on legacy systems that may not be secure.

Sanjay Sarma, one of the MIT Auto-ID Center's founders, described the problem as not IoT themselves but the "pell-mesh rush to build systems in any which way" without regard to a comprehensive security plan.⁶ The underlying challenge, Sarma explained, is that even if independent systems were secure, these systems are cobbled together, and "the chain will only be as strong as the weakest link."⁷ The software used for IoT apps also pose a problem for data security because, like the infrastructure, they "are hard to upgrade or improve" and use a "patchwork of legacy systems [such] that it is virtually impossible to replace any one without a wholesale replacement of all."⁸

Exploding Wearables Market Might Not Address Data Privacy or Security

Sensors Embedded in Wearables Allow Them to Gather Huge Amounts of Data

Wearables collect tremendous amounts of data. The technologies surrounding wearables allow that data to be used and analyzed in a variety of ways. Wearables today are embedded with more advanced technologies including microchips, sensors, and actuators. As of 2012, 3.5 billion sensors are already on the market.⁹ According to a June 2015 Lux study analyzing patents filed between 2010 and May 2015, 41,301 patents were granted for wearable electronics, and patent applications for wearable electronics are increasing at over 40 percent annually.¹⁰

Information about a person derived from wearables data such as the time, duration, and proximity of an activity to other tracked individuals combined with demographic information can provide crucial and detailed context to each individual interaction. Data gathered impacts how businesses market their products and how companies recruit talent and motivate their employees. Wearables gather a new class of sensitive data about people: not only who they are, what they do, and who they know, but also how healthy they are, what movements they make, and how well they feel.¹¹ Heart rate monitors can provide insight into people's excitement and stress levels, and glassware can reveal exactly what they are seeing. Microsoft's health-tracking wearable, Microsoft Band, incorporates exotic sensors like galvanic skin response, the same technology that is used in lie detectors. By adding heart rate and temperature information, it is now possible to make educated guesses on a user's emotional state. There is now a hands-free Tinder app for the Apple Watch that instead of allowing the user to decide consciously on a match by swiping left or right on his or her smartphone, makes the decision using the wearer's heartbeat.¹²

Consumers Demand Wearables

Great Wolf Resorts, owner of 11 water parks in North America, has used RFID wristbands since 2006 that allow the resort company to track users throughout the park and tie their activities and purchases to their names.¹³ These wristbands allow users to pay for food and beverages on account and allows them to avoid carrying money or keys on waterslides. In 2013, Walt Disney World introduced a similar vacation management system to provide users with a more customized park experience. Economist Paul Krugman cited the "Varian rule," which provides that the future can be forecasted by examining what the rich have today, supporting the idea that consumers would want resort-like experiences in their daily lives.¹⁴ For example, the *super-rich do not wait in line, rather*

"[t]hey have minions who ensure that there's a car waiting at the curb, that the maitre-d escorts them straight to their table, that there's a staff member to hand them their keys and their bags are already in the room. . . . [S]mart wristbands could replicate some of that for the merely affluent."¹⁵

Companies' Demand for Big Data Is Increasing

The European Commission's new antitrust chief, Margrethe Vestager, described data as the "new currency of the Internet." FTC Chairwoman Edith Ramirez made a similar comment: "Today's currency is data."¹⁶ Apart from consumer goodwill and trust by self-disclosing "we won't collect your data" (as Apple CEO Tim Cook has done), there is little incentive for a company not to collect data on consumers using wearables.¹⁷ A 2011 McKinsey report noted that when a competitor fails to use data and business analytics to guide decision making, it suffers competitively.¹⁸

Data collected by wearables can be analyzed to create highly targeted, individually tailored marketing campaigns. Marketers could derive from raised stress levels, poor sleep, and a combination of other behavior that a romance is in trouble. Wearable data could determine if a user was habitually late for work, largely immobile when at the office, or spent little time with his or her colleagues, and determine such behavior is due to low morale or dissatisfaction with his or her current job.

Analyzing data from wearables in conjunction with other information will allow businesses to deliver messages and services tailored to a particular customer's location, activity, and mood.¹⁹ Recruitment firms could use big data to target dissatisfied workers, and employers can use the same data to implement policy changes.²⁰ De-identified and aggregated data from wearables reveal otherwise indiscernible patterns and trends in a number of socially beneficial contexts. Medical and epidemiological research, energy conservation, and commercial productivity and efficiency are benefits of using big data.²¹ Companies can use aggregated data to have a better idea of consumer demand and develop better products and services.

Companies Innovate Independently without Addressing Data Security

In the rush to bring new wearables to market, companies may not address the data security threats. According to Cisco, by 2019, 24 billion networked devices are expected to come online (compared with 14 billion in 2014). By the end of 2012, 8.7 billion devices were connected to the Internet. That figure is expected to increase to 40 billion by 2020 as cars, refrigerators, ovens, thermostats, medical devices, and others come online.²²

IoT Innovation and Infrastructure in Healthcare Wearables

Healthcare Wearables Present the Greatest Potential for Consumer Gains

Healthcare wearables contain wireless sensors embedded in the device and worn on the body. M2M technologies and healthcare apps along with healthcare wearables could improve patient outcomes, reduce health expenditures, and allow providers to deliver care in more patient-friendly ways. For example, insulin pumps and blood-pressure cuffs that connect to mobile apps could let people record, track, and monitor their own vital signs without having to go to a doctor's office.²³ Healthcare providers can monitor patients' blood pressures, respiration rates, and a variety of other biometric information remotely and continuously thanks to wearables.

Healthcare wearables engage patients in their own care. A clinical trial of diabetic users of continuous glucose monitors showed an average blood sugar level reduction of two points; to put this finding in perspective, the FDA considers medications that reduce blood sugar by as little as one-half point to be successful.²⁴ Economist Paul Krugman said that he uses a Fitbit "because the thing spies on me all the time, and therefore doesn't let me lie to myself about my efforts."²⁵

Healthcare wearables also help medical providers better understand patient's health and healthcare issues in general. By analyzing continuous data, healthcare providers are better able to spot trends and make better decisions. In the case of continuous glucose monitors, healthcare providers can examine a patient's blood glucose levels throughout the day and over the course of their disease. Examining aggregated data, they can spot trends and better understand diabetes and how it can be controlled.²⁶

Healthcare Wearables May Pose Data Security Risks

Security risks of healthcare wearables increase with the degree of human interaction. There is a significant degree of human interaction in telehealth apps. The data captured by healthcare wearables typically flow across short, unlicensed wireless links to a monitoring hub in the patient's home, which then passes the information to the broadband network, routing it to the cloud where analytics continuously monitor a patient's status, notifying a healthcare provider in case of anomalies.²⁷ Healthcare wearables measure a patient's biometric data; an on-premises healthcare worker or a medical professional can receive the data on the other end of a wireless communications link.

In the hospital setting, medical devices have become the key points of vulnerability within healthcare networks and have been subject to attacks.²⁸ Medical devices including x-ray equipment, picture archive and communications systems, and blood gas analyzers have been the subject of cybersecurity attacks.²⁹ These attacks threaten overall hospital operations and the security of patient data. If a hospital, with a fixed infrastructure, cannot keep its medical devices secure, it is highly likely that consumers will be more vulnerable to cybersecurity attacks.

Does Government Regulation Address the Data Privacy and Security Concerns Wearables Pose?

U.S. Data Privacy Regulations Follow Fair Information Practice Principles

Even if a company follows Fair Information Practice Principles and a consumer trusts a particular company with his or her data today, those conditions may change in the future. Additionally, if a customer approves his or her data to be collected and used for a particular purpose today, that does not mean the use could be different in the future. For example, although a consumer may today use a fitness tracker solely for wellness-related purposes, the data gathered by the device could be used in the future to price health or life insurance or to infer the user's suitability for credit or employment (e.g., a conscientious exerciser is a good credit risk or will make a good employee).³⁰ Use of data for credit, insurance, and employment decisions could bring benefits—e.g., enabling safer drivers to reduce their rates for car insurance or expanding consumers' access to credit—but such uses could be problematic if they occurred without consumers' knowledge or consent, or without ensuring accuracy of the data.³¹

The Fair Credit Reporting Act (FCRA) applies to third-party consumer reports used for credit or employment purposes; it requires consent for a report to be generated and allows that report to be reviewed for inaccuracies. The FCRA excludes most "first parties" that collect consumer information. Thus, it would not generally cover IoT device manufacturers that do their own in-house analytics. Nor would the FCRA cover companies that collect data directly from consumers' connected devices and use the data to make in-house credit, insurance, or other eligibility decisions—something that could become increasingly common as IoT develops.³²

Consumers' tolerance of how companies use their data will depend on the company's transparency and how much trust the consumer has in the company with his or her data. Companies, marketers, and employers collecting data can de-identify data, but it is possible to re-identify data, especially if inadequate security

measures are in place.

Demand Side of Wearables Market May Not Be Able to Address Data Privacy and Security

Targeted ads based on data gathered from wearables could reduce marketing spam for consumers and provide them with more relevant offers. Customer service can be improved and the gulf between offline and online shopping experiences can be bridged using wearable technology. Consumers, however, are increasingly more willing to view the data privacy and security of their personal data as more important than quality of service, and are starting to give false information for access to free services.³³ The trust consumers have in a company will influence how willing they are to reveal truthful personal information and how willing they are to have their data collected.

Nest Labs is a company known for its smart thermostat that can be controlled remotely by an app. The app learns a consumer's temperature preference and when he or she is home. The app does not collect much data about the consumer apart what it needs to function. Google acquired Nest Labs in January 2014 for over \$3.2 billion in cash. Although Nest Labs has repeatedly insisted that it is not merging its data with Google's, consumers may not fully trust the company's assurances.³⁴

Users are aware of the potential data privacy implications of wearables. One study specifically found that users are aware that when data are continuously collected, stored, published, and shared, they could include information that users would not want to recall later or would not be willing to capture or be reminded of later.³⁵ Users are also aware that when data from wearables are stored in the cloud, that data could be revealed without the user's knowledge or consent. Users' data privacy concerns primarily result from devices that include cameras and microphones followed by devices with GPS and displays. Activity trackers that monitor heart rate, steps, and pulse are seen by users as inoffensive to data privacy; however, the authors of the study postured that it is likely that users are not aware of how third parties could misuse data or of the potential data privacy implications when the data are collected long term or associated with complementary information.

Conclusion

The technology supporting wearables began in a time when security risks were low and the end users were mainly businesses. Consumers have increasingly demanded technology over the past decades. Business models have changed requiring more and better consumer data. While wearables pose significant gains to consumers, especially in healthcare, a concerted effort must be

made to address privacy and security. The current technological infrastructure supporting today's wearables have not addressed the security risks. The data privacy risks have not been addressed, and there are incentives for companies to gather more data than less from consumers. Consumers have shown that they are willing to trade privacy for lower cost, more innovative products. Where the demand or supply side of the market for wearables do not address privacy, policy or self-regulation should address the data privacy and security concerns posed by wearables.

Endnotes

1. *Data, Data Everywhere*, Economist (Feb. 25, 2010), <http://www.economist.com/node/15557443>.
2. Davey Alba, *50 Years On, Moore's Law Still Pushes Tech to Double Down*, Wired (Apr. 19, 2015), <http://www.wired.com/2015/04/50-years-moores-law-still-pushes-tech-double/>.
3. Rob Stein, *Implantable Medical ID Approved by FDA*, Wash. Post, Oct. 14, 2004, <http://www.washingtonpost.com/wp-dyn/articles/A29954-2004Oct13.html>.
4. Robert McMillan, *It's Crazy What Can Be Hacked Thanks to Heartbleed*, Wired (Apr. 28, 2014), http://www.wired.com/2014/04/heartbleed_embedded/.
5. FTC Staff Report, *Internet of Things: Privacy & Security in a Connected World 20* (2015), <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>.
6. Sanjay Sarma, *I Helped Invent the Internet of Things. Here's Why I'm Worried about How Secure It Is*, Politico (June 2015), <http://www.politico.com/agenda/story/2015/06/internet-of-things-privacy-risks-security-000096>.
7. *Id.*
8. *Id.*
9. See Stanford Univ., *TSensors Summit for Trillion Sensor Roadmap* (Oct. 23–25, 2013), <http://tsensorssummit.org/Resources/Why%20TSensors%20Roadmap.pdf> [hereinafter TSensors Summit].
10. Carole Jacques, *Led by Samsung, Wearable Electronics Patents Are Growing at over 40% Annually*, Lux Res. (June 30, 2015), <http://www.luxresearchinc.com/news-and-events/press-releases/read/led-samsung-wearable-electronics-patents-are-growing-over-40>.
11. Anthony Mullen, *Fearing the Quantified Life—Privacy, Data and Wearable Devices*, The Next Web (June 5, 2015),

<http://thenextweb.com/insider/2015/06/05/fearing-the-quantified-life-privacy-data-and-wearable-devices/>.

12. Jeff Beer, *Your Heart Does the Swiping on This Hands-Free Tinder App for Apple Watch*, Fast Company (July 6, 2015), <http://www.fastcocreate.com/3048244/your-heart-does-the-swiping-on-this-hands-free-tinder-app-for-apple-watch>.

13. Theresa M. Payton & Theodore Claypoole, Privacy in the Age of Big Data 108–09 (2014).

14. Paul Krugman, *Apple and the Self-Surveillance State*, N.Y. Times, Apr. 10, 2015, http://krugman.blogs.nytimes.com/2015/04/10/apple-and-the-self-surveillance-state/?_r=4&assetType=opinion.

15. *Id.*

16. Allen P. Grunes & Maurice E. Stucke, *No Mistake About It: The Important Role of Antitrust in the Era of Big Data*, 14 Antitrust Source, no. 4, Apr. 2015, at 1, 2.

17. James Vincent, *Apple CEO Tim Cook: Unlike Other Companies, We Don't Want Your Data, Just Your Money*, Indep. (Sept. 16, 2014), <http://www.independent.co.uk/life-style/gadgets-and-tech/apple-ceo-tim-cook-unlike-other-companies-we-dont-want-your-data-just-your-money-9735212.html>.

18. Brad Brown et al., *Are You Ready for the Era of "Big Data"?*, McKinsey Q., Oct. 2011, http://www.mckinsey.com/insights/strategy/are_you_ready_for_the_era_of_big_data.

19. Mullen, *supra* note 11.

20. *Id.*

21. Comments of AT&T Inc. at 8, Workshop to Explore Privacy and Security Implications of the Internet of Things (F.T.C. May 31, 2013), *available at* https://www.ftc.gov/sites/default/files/documents/public_comments/2013/07/00004-86142.pdf.

22. See TSensors Summit, *supra* note 9.

23. FTC Staff Report, *supra* note 5, at 7.

24. *Id.*

25. Krugman, *supra* note 14.

26. Jennifer Britton-Colonnese & Devin Steenkamp, *Continuous Blood Glucose Monitoring in Newly Diagnosed Type 1 Diabetes*, Endocrinology Advisor (Jan. 9, 2015), <http://www.endocrinologyadvisor.com/diabetes/continuous-glucose-monitoring-in-type-1-diabetes/article/391865/>.

27. Comments of AT&T Inc., *supra* note 21, at 5.

28. TrapX Labs, Anatomy of an Attack: Medical Device Hijack

(MedJack) 5 (May 7, 2015).

29. *Id.* at 6.

30. FTC Staff Report, *supra* note 5, at 16.

31. *Id.*

32. *Id.* at 17.

33. Nicole Kobie, *Tech Firms Need to Use Data Ethically around the Internet of Things*, *Guardian* (June 10, 2015), <http://www.theguardian.com/technology/2015/jun/10/tech-firms-need-use-data-ethically-internet-of-things>.

34. Allison Kade, *How to Manage the Threats to Our Privacy and Financial Security in the Digital Age*, *The Street* (June 17, 2015), <http://www.thestreet.com/story/13188985/1/how-to-manage-the-threats-to-our-privacy-and-financial-security-in-the-digital-age.html>.

35. Scott Amyx, *Data Privacy Playbook for Wearables and IoT*, *InformationWeek* (June 8, 2015), <http://www.informationweek.com/mobile/mobile-devices/data-privacy-playbook-for-wearables-and-iot/a/d-id/1320690>.



Health eSource

Your Link to the ABA Health Law Section News & Information

Peeling Back the Apple Watch: Do HIPAA and the Apple Watch Go Together?

Vol. 12 No. 1

Paul A. Drey, Sarah Wendler, Brick Gentry, P.C., West Des Moines, IA



One of our more tech-savvy partners recently showed us his new Apple Watch and, instinctively, it raised questions as to how would HIPAA impact its use. Two possible answers exist to explain the rationale for the asking of such a question. The first possible answer is that one's healthcare law practice

has so embedded one's way of thinking that HIPAA concerns arise as one views most issues, or the second possible answer is that the features of this new Apple Watch may be the linchpin to a whole new culture in a mobile health industry.

Time will determine which answer is correct, but the new Apple Watch does possess some interesting features that will, at a minimum, impact the mobile healthcare industry. Along with the Apple Watch, the HealthKit app, which is an application that can be utilized by the Apple Watch and is designed to log one's activity and health data, and the ResearchKit software¹ which launched in April 2015, Apple has introduced some interesting "tools" for the healthcare marketplace for the consumer, for the provider, and possibly for other vendors. In addition to changing the healthcare marketplace, the Apple Watch and these other applications have opened the door to multiple legal issues that will need to be addressed.

Apple Watch (and Related Apps) Promise Opportunities for Consumers

The Apple Watch, launched in April 2015 along with Apple Watch Apps, have garnered much public attention.² The Apple Watch has the technology to track and store information about the activity of the wearer. It can show a person's daily activities, such as the amount of time spent sitting, standing, or moving, and it can provide and display goals, suggestions, and incentives for increased activity. The Apple Watch can also collect workout data, such as a person's heart rate, calories burned, and other exercise-related statistics. The Apple Watch is designed to track activity of the wearer through its own accelerometer and heart-rate monitor, but needs to

be paired with an iPhone to track the actual distance one travels.³ In the future, the Apple Watch may also have additional sensing and tracking capabilities.⁴ Reportedly, some of the initial sensors on the Apple Watch did not work well on people with hairy arms or with dry skin or if the Watch was fastened too loosely.⁵

Like other iPhones or mobile devices, Apple's own HealthKit app, or other apps developed by third party developers, can also be utilized on the Apple Watch. Third party developers have designed many new healthcare apps to work with the Apple Watch or have re-designed old healthcare apps to be compatible with it. The new apps tout the benefits to be offered by having the data available right on the user's wrist, whether the end-user be the healthcare consumer or the healthcare provider.⁶ Several Apple Watch apps are designed to allow the healthcare consumer to track his/her own health and to enhance communication between the consumer and his/her healthcare provider. For instance, Cerner has an app that allows patients to track their own health on their watch and to send the data to their electronic health record.⁷ Similarly, there is an app that is designed to help keep track of one's medication usage.⁸ Yet another app is designed to measure the user's blood glucose levels.⁹

Healthcare Providers May also See Opportunitites

Some of the new Apple Watch healthcare apps are designed for use by healthcare professionals and other providers. These devices are designed for rapid provider-to-provider communication and to aid in patient care. Some examples include a secure text messaging system by athenahealth, which has now been made available for the Apple Watch so that providers can communicate and sync data among their devices even more quickly.¹⁰ A Vocera clinical communication app will enable faster provider notification of important information,¹¹ and a Mayo Clinic Synthesis app will be offered that allows providers to view their schedule and basic patient information on their watch.¹² The accuracy and reliability of the measurements and healthcare information obtained from the apps over time will determine if healthcare providers can truly utilize these apps in their practice.

Privacy and Security Issues May Make the Data Vulnerable

The excitement brought to the mobile healthcare industry for consumers and providers through the Apple Watch and the many available or soon-to-be-available apps for it needs to also be met with some concern over the mechanisms in place to protect consumer privacy and especially to protect the consumer's healthcare information. The concerns include the privacy and security of the healthcare information tracked by the Apple Watch and related apps as well as the security and privacy of the storage of that healthcare information. Additional privacy and security issues arise in the transfer of the healthcare information measured by the Apple Watch from the consumer to healthcare providers and other third parties. Finally, concerns exist as to the privacy policies of the multiple third-party app vendors as each vendor has its own privacy policy, and these privacy policies vary from vendor to vendor.

There have been many recent stories in the news concerning breaches of people's private personal information, including healthcare records and health-related information. Many people assume that their healthcare information is protected through federal laws like the Health Information

Portability and Accountability Act of 1996 (HIPAA) or related laws or through the Federal Trade Commission Act (the FTC Act). HIPAA as well as subsequent laws, such as the Health Information Technology for Economic and Clinical Health Act (HITECH), are designed to provide privacy and security protections to an individual's protected health information. The FTC Act, Section 5, prohibits unfair or deceptive acts or practices which affect or impact commerce.¹³ The Federal Trade Commission (FTC) has also actively attempted to regulate patient information or healthcare data and the security practices or safeguards of the companies participating in commerce.¹⁴ In addition, the FTC will take action if an app claims benefits or promises to consumers if such healthcare claims are not based on sound science.¹⁵

Applicability of HIPAA

Interestingly, the application of laws like HIPAA to the Apple Watch and its related apps is not clear. One of the major potential privacy concerns is that current healthcare privacy laws, like HIPAA, do not address healthcare data stored on a consumers' own personal device.¹⁶ The coverage of HIPAA and related laws to the data collected by the Apple Watch depends on who is storing and using the data, as well as to the creation, maintenance, reception and transmission of the data. To the extent that the healthcare data stored on the Apple Watch and used in a health app is "protected health information" and is used by or in the control of a "covered entity" or used by its "business associate," then the framework of HIPAA obligations and restrictions would exist to protect the health data. HIPAA defines a "covered entity" as "(1) health plans, (2) healthcare clearinghouses, and (3) healthcare providers who electronically transmit any health information in connection with a transaction covered by this subchapter [at HIPAA]." ¹⁷ HIPAA defines a "business associate" as "a person who on behalf of such covered entity or of an organized healthcare arrangement in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter" ¹⁸ An example of such a case would be when a user (a patient of Mayo) transmits health data from an Apple Watch or health app to the Mayo Clinic App. At the point the health data is received by Mayo, since Mayo qualifies as a covered entity under HIPAA, then the health data qualifies as protected health information and is HIPAA-protected. Similarly, athenahealth's new text app for the Apple Watch is also promoted as a means for providers to have a more uniform and centralized method of communication that is secure and complies with HIPAA requirements, rather than resorting to a variety of traditional and less secure methods.¹⁹ Given the number of new health apps that are designed for healthcare professionals and have already been created or are likely to be created in the future for the Apple Watch, it will be important for each covered entity and business associate to understand how HIPAA applies to the design and use of the app and how patient health data is used, maintained and stored.

Another question is whether Apple or other vendors with a role in the app or the storage or transmission of the health data come under the purview of HIPAA as a "business associate."²⁰ These entities would be considered business associates if they create, receive, maintain, or transmit protected

health information on behalf of a covered entity. The determining factor hinges upon how the health data flows, but if a covered entity provides “the protected health information to a vendor, for claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety, activities [...], billing, benefit management, practice management, and repricing,” then it is a business associate.²¹ Thus, an app that receives protected health information from a covered entity and then analyzes the data is a business associate and subject to HIPAA.

Questions of the adequacy of privacy controls also arise when the data is simply stored on the user’s wearable or hand-held device, or when the user uploads the data to a third-party health or fitness app that is not covered by HIPAA. It should be noted that Apple has taken some proactive steps to safeguard the privacy of its consumers’ health data. Apple’s HealthKit framework that allows apps to obtain health data from the user’s device has specific privacy parameters in place, but it still raises issues as to the apps with which health information is shared.²² Apple claims that it builds privacy protections into its devices and apps.²³

For covered entities and business associates, it will be important to understand how their use of the Apple Watch and related apps to obtain patient information is covered by HIPAA and to ensure that their privacy practices and uses and disclosures of the health information comply with HIPAA requirements. App developers will likely still have to develop and follow a privacy policy, even if they are not regulated under HIPAA. They also need to consider whether individual state privacy laws have any requirements applicable to them. Finally, consumer demand for privacy may also dictate the increase in privacy policy concerning the Apple Watch and similar mobile devices.

Applicability of the FTC

The FTC has actively shown interest in determining and scrutinizing how the increasing amount of consumer-generated health and fitness data will be safeguarded by companies involved in that relevant sector.²⁴ In particular, the FTC has expressed concerns about the “risks of health data that flows outside of a medical context, such as information collected via wearables and mobile health apps,” and such concerns have prompted discussions with Apple.²⁵ As a result, it has been reported that Apple requires that its users must give consent before app developers are given access to the health information and further, that “data logged by its smartwatch is encrypted.”²⁶ Apple has taken steps to ensure that personal health information obtained through its HealthKit app is not used by developers for advertising or other non-consented purposes, but the FTC remains concerned as to whether Apple will be able to ensure that apps follow the same rule and take the same safeguards.²⁷ It is very likely that the FTC will continue to monitor and review future mobile health developments.

Apple Watch Raises Other Concerns

The Apple Watch and similar mobile devices in healthcare also raises patient safety concerns. Recently, the specter of patient safety in using these devices in order to make medical determinations has been raised. For instance, early reports of the Apple Watch indicated that it might be able to detect heart attacks, or measure health metrics, such as glucose levels, which would raise the concern of Food and Drug Administration

(FDA). However, the Apple Watch appears to be more in line to motivate its wearer to take action to stay healthy versus monitoring the healthcare vitals of the user, so the FDA is less likely to get too involved.²⁸ If more healthcare features are added, then the FDA may become more aggressive.²⁹ FDA regulation of mobile medical apps is evolving.³⁰

Another concern to consider is how health-related data used in an app or stored on an Apple Watch could be obtained through legal e-discovery procedures.³¹ Will the information stored on your Apple Watch become evidence in a legal proceeding? Time will provide judges the opportunity to rule on these discovery/evidentiary issues.

Conclusion

The Apple Watch is neither the first mobile device with capabilities and features that are applicable to healthcare delivery and/or care coordination, nor is it the first wearable device. However, given the potential widespread use and visibility of this and similar such watch devices by healthcare professionals and consumers, the Apple Watch could play a major role in the development of the mobile healthcare industry and have an impact on the regulatory framework used to control patient privacy. Before using the Apple Watch or other wearable devices for their healthcare needs and sharing their sensitive health data, consumers will need to be aware that different apps will have different privacy policies and that not all health apps will be compliant with HIPAA or FTC requirements. It will also be important for regulators and industry experts to understand the capabilities of the wearable devices and all of the new health apps and how their use impacts consumer privacy and to continue to monitor as these features change rapidly. The Apple Watch, peeled back, has provided the core to this mobile health evolution.

Paul Drey is a shareholder and the Managing Partner at Brick Gentry P.C., who practices primarily in the areas of healthcare and business/commercial/transactional/corporate law. Mr. Drey is an established advisor to his healthcare clients, including medical groups, physicians and other medical/healthcare associations. His experience includes advising on entity structures, healthcare transactions, physician contracts, recruiting, personal services and employment, business plans, ACO arrangements, regulatory compliance, including STARK, HIPAA, HITECH, and other healthcare-related areas of law. Mr. Drey authors the blog, [Iowa Healthcare Law Blog](#). He may be reached at brickgentrylaw.com.

Sarah J. Wendler is an associate at Brick Gentry P.C. in West Des Moines, Iowa, who focuses her practice primarily in the areas of corporate law and general business law, including the areas of healthcare and agricultural law. Her experience includes advising clients on a variety of corporate and transactional matters and assisting partners in the Healthcare Section at Brick Gentry on a diverse range of healthcare-related matters. She may be reached at sarah.wendler@brickgentrylaw.com.

¹ <http://www.technologytell.com/apple/147612/apple-watch-researchkit/>;
<https://www.newscientist.com/article/dn27123-Apple-researchkit-and-watch-will-boost-health-research/>.

<http://www.mhealthnews.com/print/30421>.

3 <http://www.wired.com/2014/09/apple-watch-fitness-apps/>.

4 <http://www.fiercemobilehealthcare.com/story/health-functions-dropped-apple-watch-after-glitches/2015-02-18>; and see also <http://mobihealthnews.com/40610/report-accuracy-concerns-led-apple-to-cut-advanced-health-features-from-apple-watch/>.

5 *Id.*

6 <http://healthcareitnews.com/news/health-tools-apple-watch-arrive>;
<http://healthdatamanagement.com/news/Vendors-Organizations-Start-Cranking-Out-Apple-Watch-Apps-50263-1.html>.

7 <http://cerner.com/Cerner-Announces-Apple-Watch-App/>.

8 <http://www.medisafe.com>.

9 <http://www.fiercemobilehealthcare.com/story/diabetes-tracking-app-development-apple-watch/2015-02-11>.

10 <http://newsroom.athenahealth.com/phoenix.zhmtl?c=253091&p=irol-newsArticle&ID=2034057>.

11 <http://www.vocera.com/press-release/vocera-announces-first-clinical-commnications-app-apple-watch>.

12 <http://www.apple.com/watch/app-store-apps/>.

13 <http://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf>.

14 <http://www.govhealthit.com/news/cor-ftc-regulate-digital-health-privacy>.

15 <https://www.washingtonpost.com/news/the-switch/wp/2015/09/17/apps-are-making-health-claims-but-they-may-not-have-the-science-to-back-them-up/>.

16 <https://www.washingtonpost.com/news/the-switch/wp/2015/09/17/apps-are-making-health-claims-but-they-may-not-have-the-science-to-back-them-up/>.

17 45 C.F.R. 160.103 – Definitions.

18 45 C.F.R. 160.103 – Definitions.

19 <http://www.athenahealth.com/blog/2015/04/12/athenatext-meet-apple-watch>.

20 <http://www.reuters.com/article/2014/08/12/us-apple-healthcare-exclusive-idUSKBN0GC09K20140812>.

21 42 C.F.R. 160.103 – Definitions.

22 https://developer.apple.com/library/ios/documentation/HealthKit/Reference/HealthKit_Framework/;
http://www.leadingage.org/Are_Apple_HealthKit_Customers_Trading_Privacy_for_Health.aspx.

- 23 <http://www.apple.com/privacy/privacy-built-in/>.
- 24 <http://www.reuters.com/article/2014/11/13/us-apple-ftc-exclusive>.
- 25 *Id.*; <http://mobihealthnews.com/38315/report-ftc-apple-discuss-apple-watch-and-health-data-privacy>.
- 26 *Id.*
- 27 <http://www.macworld.com/article/284802/apple-watch-health-apps-may-already-be-under-ftc-microscope>; *Id.*
- 28 <http://bgr.com/2015/03/30/apple-watch-fda-scrutiny>.
- 29 *Id.*
- 30 <http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/ConnectedHealth?mobileMedicalApplications/default.htm>.
- 31 <http://www.blogs.findlaw.com/technologist/2014/11/ftc-concerned-about-apple-watch-3rd-party-access-to-health-info.html>; <http://blogs.wsj.com/digits/2014/09/09/as-apple-moves-into-health-apps-what-happens-to-privacy/>.

BUSINESS DAY

Neiman Marcus Data Breach Worse Than First Said

By ELIZABETH A. HARRIS, NICOLE PERLROTH and NATHANIEL POPPER JAN. 23, 2014

The theft of consumer data from Neiman Marcus appears far deeper than had been disclosed originally, with the luxury retailer now saying that hackers invaded its systems for several months in a breach that involved 1.1 million credit and debit cards.

The malware installed on terminals in Neiman Marcus stores seems to be the same malware that infiltrated Target's systems and exposed information from as many as 110 million customers, according to a person briefed on the investigations who spoke on the condition of anonymity and is not authorized to speak publicly about the attacks.

Investigators have not revealed whether the same cybercriminals are suspected in both breaches, although investigators and security specialists have described a loose band of hackers from Eastern Europe as the likeliest suspects in the Target theft. Security specialists working with the authorities have said that the hackers were considering several major retailers as potential targets.

In a statement posted on its website Wednesday night, Neiman Marcus said that the malware had been "clandestinely" put into its system and had stolen payment data off cards used from July 16 to Oct. 30. MasterCard, Visa and Discover have told the company that about 2,400 cards used at Neiman Marcus and its Last Call outlet stores have since been used fraudulently.

The Neiman Marcus Group, which also owns Bergdorf Goodman, has said it was not aware of the data theft until mid-December, when a payment processor reported that unauthorized charges were showing up on cards used at its stores. It now plans to notify all customers who shopped in those stores from January 2013 to this month — and for whom the company has a mailing or email address. Like Target, it said it would offer those shoppers one free year of credit monitoring.

In the instances of widespread data theft at Target and Neiman Marcus, the malware was designed to hook into cash registers to monitor the credit card authorization process. Before a transaction can be authorized, credit card data is momentarily decrypted and stored in memory. Called RAM-scraping malware, it is built to scrape that unencrypted data from memory and steal it, according to a private report issued by iSight Partners, which is working with the Department of Homeland Security to investigate the retail attacks.

The data thefts have reignited a push for more secure credit and debit cards, similar to those used in Europe and elsewhere, and have prompted some congressional committees and senators to renew calls for tougher consumer protections.

In addition to an investigation of the breach by the Secret Service, the Justice Department and several state attorneys general, the Senate Judiciary Committee has asked Target for documents related to its cybersecurity efforts and the malware used in the attack. Target's chief financial officer, John J. Mulligan, will be the first witness to appear before the committee at a hearing on Feb. 4. Federal authorities also are expected to testify.

Since the Target breach in November, the attention of retailers and the card industry has turned to EMV technology, named for its founders, Eurocard, MasterCard and Visa. Cards using the technology have a small chip embedded that creates a new code for each transaction, making it nearly impossible to counterfeit the cards in the way that has happened since card numbers were stolen from Target.

“EMV wouldn't have stopped it, but it would have helped minimize the impact after the event,” according to Don Tait, an analyst at IHS.

The United States is one of the last countries to move toward the technology. In Europe, 81 percent of the cards have EMV chips, according to the consulting firm Celent. Countries that have adopted the technology have seen a sharp decline in credit card fraud. In Britain the amount of fraud per transaction has dropped 57 percent since 2002. Meanwhile, fraud has risen sharply in the United States, some 70 percent between 2004 and 2010, Celent information shows.

While the United States accounts for only 27 percent of the credit card transactions in the world, it is responsible for 47 percent of card fraud, according to data from the Nilson Report, a newsletter about the payment industry.

“The rest of the world is onto new technology, and we’re still using magnetic stripe technology that was used for eight track tape players in the 1960s,” Chris McWilton, a MasterCard executive, said on Thursday. “No wonder the fraudsters have found us.”

The United States has not moved faster because retailers and card issuers have worried that the cost of adopting the technology, usually estimated at \$15 billion to \$30 billion, would be more than the cost of the fraud it prevented. Even with increasing fraud in the United States, it has only cost about 5 cents for every \$100 of credit card use.

The main proponents of change have been the major card companies. Visa, MasterCard and American Express have all said that American retailers need to install hardware that can read EMV cards by October 2015. Any retailers that do not, and have data stolen, will be liable for the costs of any fraud.

In the last year, retailers complained frequently about the costs of shifting to another technology. In October, a Visa executive hinted that the company was listening to the retailers and considering revising its schedule. Regulatory changes, meanwhile, have muddied the waters of how chip technology could be applied uniformly.

“There was a clear apathy in the industry,” said Zilvinas Bareisis, a card analyst at Celent, said of the retailers’ reluctance.

But now, many players, including the Target chief executive Gregg W. Steinhafel, have talked about the importance of moving to EMV. In a letter this month, MasterCard told its clients it was recommitting itself to making the transition happen by 2015.

“It’s been a wake-up call,” Mr. McWilton said in an interview. “There were a lot of naysayers and people satisfied with the status quo. Now, I think, people have woken up and said, ‘If you don’t have the public trust, you don’t have the business.’ ”

Investors are betting that the revived interest in new technology will lead to changes. The stock of companies that would manufacture some of the new technology has been pushed up since the Target breach. Verifone, the most prominent manufacturer of payment hardware, is up 27 percent over the last month.

But card issuers have been careful to point out that cards with chips will not stamp out all fraud. The chips do not prevent card numbers from being used fraudulently online, and in Britain that sort of crime has risen even while overall fraud has dropped. On that front, many financial firms have been pushing the idea of tokenization, which creates a new code for each transaction, making it hard to use the same card repeatedly. Mr. Bareisis said it could be a problem if the United States adopted only one part of the antifraud technology available.

Recently, smaller instances of customer data theft have surfaced at other retailers, as well.

Nordstrom said it found skimming devices on 10 registers at a store in Miami in October, which stripped information like account numbers and expiration dates off cards. (A company spokeswoman said that the attack appeared to have been confined to just those machines and that the company had no evidence its system was breached.) And this week, Easton-Bell Sports said 6,000 people who shopped at its online store in December had their information compromised, including names, email addresses, credit card numbers or card security codes.

Criminal demand for the kind of point-of-sale malware used in the attacks on Target and Neiman Marcus has been steadily growing. Security specialists say cybercriminals will post advertisements on online freelancing sites looking for help

in developing point-of-sale malware. Last July, on a popular freelancing site, security researchers at iSight Partners found that more than 20 percent of all ads appeared to be from criminals looking to hire hackers with expertise in point-of-sale systems.

And hackers that have expertise in point-of-sale systems have been increasing their rates. Early in 2010, hackers were charging \$425 to \$2,500 for point-of-sale malware projects. By the end of the year, their rates had spiked to \$6,500, according to a report prepared by iSight Partners

Though most point-of-sale malware developers are based in Eastern Europe, security researchers say that cybercriminals in Brazil have been developing and using point-of-sale malware since at least 2009.

A version of this article appears in print on January 24, 2014, on page B1 of the New York edition with the headline: Neiman Marcus Data Breach Worse Than First Said.

**PREPARED STATEMENT OF
THE FEDERAL TRADE COMMISSION**

on

Data Breach on the Rise: Protecting Personal Information From Harm

Before the

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

UNITED STATES SENATE

Washington, D.C.

April 2, 2014

I. INTRODUCTION

Chairman Carper, Ranking Member Coburn, and members of the Committee, I am Edith Ramirez, Chairwoman of the Federal Trade Commission (“FTC” or “Commission”).¹ I appreciate the opportunity to present the Commission’s testimony on data security, and for your leadership, Chairman Carper, on this important issue.

Consumers’ data is at risk. Recent publicly announced data breaches² remind us that hackers and others seek to exploit vulnerabilities, obtain unauthorized access to consumers’ sensitive information, and potentially misuse it in ways that can cause serious harm to consumers as well as businesses. These threats affect more than payment card data; breaches reported in recent years have also compromised Social Security numbers, account passwords, health data, information about children, and other types of personal information.

Data security is of critical importance to consumers. If companies do not protect the personal information they collect and store, that information could fall into the wrong hands, resulting in fraud, identity theft, and other harm, along with a potential loss of consumer confidence in the marketplace. As one example, the Bureau of Justice Statistics estimates that 16.6 million persons – or 7 percent of all U.S. residents ages 16 and older – were victims of identity theft in 2012.³

¹ This written statement presents the views of the Federal Trade Commission. My oral statements and responses to questions are my own and do not necessarily reflect the views of the Commission or of any other Commissioner.

² See Elizabeth A. Harris & Nicole Perlroth, *For Target, the Breach Numbers Grow*, N.Y. Times, Jan. 10, 2014, available at <http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html> (discussing recently-announced breaches involving payment card information by Target and Neiman Marcus); Nicole Perlroth, *Michaels Stores Is Investigating Data Breach*, N.Y. Times, Jan. 25, 2014, available at <http://www.nytimes.com/2014/01/26/technology/michaels-stores-is-investigating-data-breach.html> (announcement of potential security breach involving payment card information).

³ See Bureau of Justice Statistics, *Victims of Identity Theft, 2012* (Dec. 2013), available at <http://www.bjs.gov/content/pub/pdf/vit12.pdf>.

As the nation's leading privacy enforcement agency, the Commission has undertaken substantial efforts for over a decade to promote data security and privacy in the private sector through civil law enforcement, education, and policy initiatives. The Commission is here today to reiterate its longstanding, bipartisan call for enactment of a strong federal data security and breach notification law. Never has the need for legislation been greater. With reports of data breaches on the rise, and with a significant number of Americans suffering from identity theft, Congress must act. This testimony provides an overview of the Commission's data security efforts, and restates the FTC's support for data security legislation.

II. THE COMMISSION'S DATA SECURITY PROGRAM

A. Law Enforcement

The Commission enforces several statutes and rules that impose obligations upon businesses to protect consumer data. The Commission's Safeguards Rule, which implements the Gramm-Leach-Bliley Act ("GLB Act"), for example, provides data security requirements for non-bank financial institutions.⁴ The Fair Credit Reporting Act ("FCRA") requires consumer reporting agencies to use reasonable procedures to ensure that the entities to which they disclose sensitive consumer information have a permissible purpose for receiving that information,⁵ and imposes safe disposal obligations on entities that maintain consumer report information.⁶ The Children's Online Privacy Protection Act (COPPA) requires reasonable security for children's information collected online.⁷ Reasonableness is the foundation of the data security provisions of each of these laws.

⁴ 16 C.F.R. Part 314, implementing 15 U.S.C. § 6801(b).

⁵ 15 U.S.C. § 1681e.

⁶ *Id.* at § 1681w. The FTC's implementing rule is at 16 C.F.R. Part 682.

⁷ 15 U.S.C. §§ 6501-6506; *see also* 16 C.F.R. Part 312 ("COPPA Rule").

In addition, the Commission enforces the proscription against unfair or deceptive acts or practices in Section 5 of the FTC Act.⁸ A company acts deceptively if it makes materially misleading statements or omissions.⁹ Using its deception authority, the Commission has settled more than 30 matters challenging companies' express and implied claims about the security they provide for consumers' personal data. Further, a company engages in unfair acts or practices if its data security practices cause or are likely to cause substantial injury to consumers that is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or to competition.¹⁰ The Commission has settled more than 20 cases alleging that a company's failure to reasonably safeguard consumer data was an unfair practice.¹¹

The FTC conducts its data security investigations to determine whether a company's data security measures are reasonable and appropriate in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities. The Commission's 50 settlements with businesses that it charged with failing to provide reasonable protections for consumers' personal information have halted harmful data security practices; required companies to accord strong protections for consumer data; and raised awareness about the risks to data, the need for reasonable and appropriate security, and the types of security failures that raise concerns.¹² And they have addressed the risks to a wide variety of consumer data, such as Social Security

⁸ 15 U.S.C. § 45(a).

⁹ See Federal Trade Commission Policy Statement on Deception, appended to *Cliffdale Assocs., Inc.*, 103 F.T.C. 110, 174 (1984).

¹⁰ See Federal Trade Commission Policy Statement on Unfairness, appended to *Int'l Harvester Co.*, 104 F.T.C. 949, 1070 (1984) ("FTC Unfairness Statement").

¹¹ Some of the Commission's data security settlements allege both deception and unfairness, as well as allegations under statutes such as the FCRA, GLB Act, and COPPA.

¹² See Commission Statement Marking the FTC's 50th Data Security Settlement, Jan. 31, 2014, available at <http://www.ftc.gov/system/files/documents/cases/140131gmrstatement.pdf>.

numbers, health data, data about children, credit card information, bank account information, usernames, and passwords, in a broad range of sectors and platforms.

In each of these cases, the Commission has examined a company's practices as a whole and challenged alleged data security failures that were multiple and systemic. Through these settlements, the Commission has made clear that reasonable and appropriate security is a continuous process of assessing and addressing risks; that there is no one-size-fits-all data security program; that the Commission does not require perfect security; and that the mere fact that a breach occurred does not mean that a company has violated the law.

In its most recent cases, the FTC entered into settlements with Credit Karma¹³ and Fandango¹⁴ to resolve allegations that the companies misrepresented the security of their mobile applications ("apps"). Credit Karma's mobile app allows consumers to monitor and access their credit scores, credit reports, and other credit report and financial data, and has been downloaded over one million times. Fandango's mobile app has over 18.5 million downloads and allows consumers to purchase movie tickets. According to the complaints, despite claims that the companies provided reasonable security to consumers' data, Credit Karma and Fandango did not securely transmit consumers' sensitive personal information through their mobile apps. In particular, the apps failed to authenticate and secure the connections used to transmit this data, and left consumers' information vulnerable to exposure – including Social Security numbers, birthdates, and credit report information in the Credit Karma app, and credit card information in the Fandango app. The Commission's settlement agreements prohibit Credit Karma and Fandango from making misrepresentations about privacy and security, and require the companies

¹³ *Credit Karma, Inc.*, No. 132-3091 (F.T.C. March 28, 2014) (proposed consent agreement), available at <http://www.ftc.gov/enforcement/cases-proceedings/132-3091/credit-karma-inc>.

¹⁴ *Fandango, LLC*, No. 132-3089 (F.T.C. March 28, 2014) (proposed consent agreement), available at <http://www.ftc.gov/enforcement/cases-proceedings/132-3089/fandango-llc>.

to implement comprehensive information security programs and undergo independent audits for the next 20 years.

The FTC also recently announced a case against TRENDnet, which involved a video camera designed to allow consumers to monitor their homes remotely.¹⁵ The complaint alleges that TRENDnet marketed its SecurView cameras for purposes ranging from home security to baby monitoring. Although TRENDnet claimed that the cameras were “secure,” they had faulty software that left them open to online viewing, and in some instances listening, by anyone with the cameras’ Internet address. This resulted in hackers posting 700 consumers’ live feeds on the Internet. Under the FTC settlement, TRENDnet must maintain a comprehensive security program, obtain outside audits, notify consumers about the security issues and the availability of software updates to correct them, and provide affected customers with free technical support for the next two years.

The FTC also has brought a number of cases alleging that unreasonable security practices allowed hackers to gain access to consumers’ credit and debit card information, leading to many millions of dollars of fraud loss.¹⁶ The Commission’s settlement with TJX provides a good example of the FTC’s examination of reasonableness in the data security context.¹⁷ According to the complaint, TJX engaged in a number of practices that, taken together, failed to reasonably protect consumer information. Among other things, it (1) failed to implement measures to limit

¹⁵ *TRENDnet, Inc.*, No. C-4426(F.T.C. Jan. 16, 2014) (consent order), available at <http://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter>.

¹⁶ See, e.g., *Dave & Buster’s, Inc.*, No. C-4291 (F.T.C. May 20, 2010) (consent order), available at <http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2010/06/dave-busters-incin-matter>; *DSW, Inc.*, No. C-4157 (F.T.C. Mar. 7, 2006) (consent order), available at <http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2006/03/dsw-incin-matter>; *BJ’s Wholesale Club, Inc.*, No. C-4148 (F.T.C. Sept. 20, 2005) (consent order), available at <http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2005/09/bjs-wholesale-club-inc-matter>.

¹⁷ *The TJX Cos., Inc.*, No. C-4227 (F.T.C. July 29, 2008) (consent order), available at <http://www.ftc.gov/enforcement/cases-and-proceedings/cases/2008/08/tjx-companies-inc-matter>.

wireless access to its stores, allowing a hacker to connect wirelessly to its networks without authorization; (2) did not require network administrators to use strong passwords; (3) failed to use a firewall or otherwise limit access to the Internet on networks processing cardholder data; and (4) lacked procedures to detect and prevent unauthorized access, such as by updating antivirus software and responding on security warnings and intrusion alerts. As a result, a hacker obtained tens of millions of credit and debit payment cards, as well as the personal information of approximately 455,000 consumers who returned merchandise to the stores. As this matter illustrates, the FTC's approach to reasonableness looks to see whether companies have implemented basic, fundamental safeguards that are reasonable and appropriate in light of the sensitivity and volume of the data it holds, the size and complexity of its data operations, and the cost of available tools.

B. Policy Initiatives

The Commission also undertakes policy initiatives to promote privacy and data security. For example, the FTC hosts workshops on business practices and technologies affecting consumer data. The FTC is in the midst of hosting its Spring Privacy Series to examine the privacy implications of a number of new technologies in the marketplace.¹⁸ The first seminar, held in February, included a panel of industry, technical experts, and privacy advocates and examined the privacy and security implications of mobile device tracking, where retailers and other companies rely on technology that can reveal information about consumers' visits to and movements within a location.¹⁹

¹⁸ Press Release, *FTC to Host Spring Seminars on Emerging Consumer Privacy Issues*, Dec. 2, 2013, available at <http://www.ftc.gov/news-events/press-releases/2013/12/ftc-host-spring-seminars-emerging-consumer-privacy-issues>.

¹⁹ See Spring Privacy Series, *Mobile Device Tracking*, Feb. 19, 2014, available at <http://www.ftc.gov/news-events/events-calendar/2014/02/spring-privacy-series-mobile-device-tracking>.

In November, the FTC held a workshop on the phenomenon known as the “Internet of Things” – *i.e.*, Internet-connected refrigerators, thermostats, cars, and other products and services that can communicate with each other and/or consumers.²⁰ The workshop brought together academics, industry representatives, and consumer advocates to explore the security and privacy issues from increased connectivity in everyday devices, in areas as diverse as smart homes, connected health and fitness devices, and connected cars. Commission staff is developing a report on privacy and security issues raised at the workshop and in the public comments.

And last June, the Commission hosted a public forum on mobile security issues, including potential threats to U.S. consumers and possible solutions to them.²¹ As the use of mobile technology increases at a rapid rate and consumers take advantage of the technology’s benefits in large numbers, it is important to address threats that exist today as well as those that may emerge in the future. The forum brought together technology researchers, industry members and academics to explore the security of existing and developing mobile technologies and the roles various members of the mobile ecosystem can play in protecting consumers from potential security threats.

C. Consumer Education and Business Guidance

The Commission is also committed to promoting better data security practices through consumer education and business guidance. On the consumer education front, the Commission sponsors OnGuard Online, a website designed to educate consumers about basic computer security.²² OnGuard Online and its Spanish-language counterpart, Alerta en Línea,²³ average

²⁰ FTC Workshop, *Internet of Things: Privacy & Security in a Connected World* (Nov. 19, 2013), available at <http://www.ftc.gov/bcp/workshops/internet-of-things/>.

²¹ FTC Workshop, *Mobile Security: Potential Threats and Solutions* (June 4, 2013), available at <http://www.ftc.gov/bcp/workshops/mobile-security/>.

²² See <http://www.onguardonline.gov>.

more than 2.2 million unique visits per year. Also, for consumers who may have been affected by the recent Target and other breaches, the FTC posted information online about steps they should take to protect themselves.²⁴

The Commission directs its outreach to businesses as well to provide education about applicable legal requirements and reasonable security practices. For example, the FTC widely disseminates its business guide on data security,²⁵ along with an online tutorial based on the guide.²⁶ These resources are designed to provide a variety of businesses – and especially small businesses – with practical, concrete advice as they develop data security programs and plans for their companies. First, companies should know what consumer information they have and what personnel or third parties have, or could have, access to it. Understanding how information moves into, through, and out of a business is essential to assessing its security vulnerabilities. Second, companies should limit the information they collect and retain based on their legitimate business needs, so that needless storage of data does not create unnecessary risks of unauthorized access to the data. Third, businesses should protect the information they maintain by assessing risks and implementing protections in certain key areas – physical security, electronic security, employee training, and oversight of service providers. Fourth, companies should properly

²³ See <http://www.alertaenlinea.gov>.

²⁴ See Nicole Vincent Fleming, *An Unfortunate Fact About Shopping*, FTC Consumer Blog, <http://www.consumer.ftc.gov/blog/unfortunate-fact-about-shopping> (Jan. 27, 2014); Nicole Vincent Fleming, *Are you affected by the recent Target hack?*, FTC Consumer Blog, <https://www.consumer.ftc.gov/blog/are-you-affected-recent-target-hack>. In addition to these materials posted in response to recent breaches, the FTC has long published a victim recovery guide and other resources to explain the immediate steps identity theft victims should take to address the crime; how to obtain a free credit report and correct fraudulent information in credit reports; how to file a police report; and how to protect their personal information. See <http://www.consumer.ftc.gov/features/feature-0014-identity-theft>.

²⁵ See *Protecting Personal Information: A Guide for Business*, available at <http://business.ftc.gov/documents/bus69-protecting-personal-information-guide-business>.

²⁶ See *Protecting Personal Information: A Guide for Business (Interactive Tutorial)*, available at <http://business.ftc.gov/multimedia/videos/protecting-personal-information>.

dispose of information that they no longer need. Finally, companies should have a plan in place to respond to security incidents, should they occur.

The Commission has also released articles directed towards a non-legal audience regarding basic data security issues for businesses.²⁷ For example, because mobile apps and devices often rely on consumer data, the FTC has developed specific security guidance for mobile app developers as they create, release, and monitor their apps.²⁸ The FTC also creates business educational materials on specific topics – such as the risks associated with peer-to-peer (“P2P”) file-sharing programs and companies’ obligations to protect consumer and employee information from these risks²⁹ and how to properly secure and dispose of information on digital copiers.³⁰

III. DATA SECURITY LEGISLATION

The FTC supports federal legislation that would (1) strengthen its existing authority governing data security standards on companies and (2) require companies, in appropriate circumstances, to provide notification to consumers when there is a security breach.³¹

²⁷ See generally <http://www.business.ftc.gov/privacy-and-security/data-security>.

²⁸ See *Mobile App Developers: Start with Security* (Feb. 2013), available at <http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security>.

²⁹ See *Peer-to-Peer File Sharing: A Guide for Business* (Jan. 2010), available at <http://business.ftc.gov/documents/bus46-peer-peer-file-sharing-guide-business>.

³⁰ See *Copier Data Security: A Guide for Business* (Nov. 2010), available at <http://business.ftc.gov/documents/bus43-copier-data-security>.

³¹ See, e.g., Prepared Statement of the Federal Trade Commission, “Privacy and Data Security: Protecting Consumers in the Modern World,” Before the Senate Committee on Commerce, Science, and Transportation, 112th Cong., June 29, 2011, available at http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-privacy-and-data-security-protecting-consumers-modern/110629privacystatementbrill.pdf; Prepared Statement of the Federal Trade Commission, “Data Security,” Before Subcommittee on Commerce, Manufacturing, and Trade of the House Committee on Energy and Commerce, 112th Cong., June 15, 2011, available at http://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-data-security/110615datasecurityhouse.pdf; FTC, *Security in Numbers, SSNs and ID Theft* (Dec. 2008), available at <http://www.ftc.gov/sites/default/files/documents/reports/security-numbers-social-security-numbers-and->

Reasonable and appropriate security practices are critical to preventing data breaches and protecting consumers from identity theft and other harm. Where breaches occur, notifying consumers helps them protect themselves from any harm that is likely to be caused by the misuse of their data. For example, in the case of a breach of Social Security numbers, notifying consumers will enable them to request that fraud alerts be placed in their credit files, obtain copies of their credit reports, scrutinize their monthly account statements, and take other steps to protect themselves. And although most states have breach notification laws in place, having a strong and consistent national requirement would simplify compliance by businesses while ensuring that all consumers are protected.

Legislation in both areas – data security and breach notification – should give the FTC the ability to seek civil penalties to help deter unlawful conduct, jurisdiction over non-profits, and rulemaking authority under the Administrative Procedure Act. Under current laws, the FTC only has the authority to seek civil penalties for data security violations with regard to children’s online information under COPPA or credit report information under the FCRA.³² To help ensure effective deterrence, we urge Congress to allow the FTC to seek civil penalties for all data security and breach notice violations in appropriate circumstances. Likewise, enabling the FTC to bring cases against non-profits³³ would help ensure that whenever personal information is collected from consumers, entities that maintain such data adequately protect it.³⁴

[identity-theft-federal-trade-commission-report/p075414ssnreport.pdf](http://www.ftc.gov/sites/default/files/documents/reports/presidents-identity-theft-task-force-report/081021taskforcereport.pdf); President’s Identity Theft Task Force, *Identity Theft Task Force Report* (Sept. 2008), available at <http://www.ftc.gov/sites/default/files/documents/reports/presidents-identity-theft-task-force-report/081021taskforcereport.pdf>.

³² The FTC can also seek civil penalties for violations of administrative orders. 15 U.S.C. § 45(l).

³³ Non-profits are generally outside the FTC’s jurisdiction. 15 U.S.C. §§ 44 & 45(a).

³⁴ A substantial number of reported breaches have involved non-profit universities and health systems. See Privacy Rights Clearinghouse Chronology of Data Breaches (listing breaches including breaches at non-profits, educational institutions, and health facilities), available at <http://www.privacyrights.org/data-breach/new>.

Finally, rulemaking authority under the Administrative Procedure Act would enable the FTC in implementing the legislation to respond to changes in technology. For example, whereas a decade ago it would be incredibly difficult and expensive for a company to track an individual's precise geolocation, the explosion of mobile devices has made such information readily available. And, as the growing problem of child identity theft has brought to light in recent years, a child's Social Security number alone can be combined with another person's information, such as name or date of birth, in order to commit identity theft.³⁵ Rulemaking authority would allow the Commission to ensure that as technology changes and the risks from the use of certain types of information evolve, companies would be required to give adequate protection to such data.

IV. CONCLUSION

Thank you for the opportunity to provide the Commission's views on data security. The FTC remains committed to promoting reasonable security for consumer data and we look forward to continuing to work with the Committee and Congress on this critical issue.

³⁵ FTC Workshop, *Stolen Futures: A Forum on Child Identity Theft* (July 12, 2011), available at <http://www.ftc.gov/news-events/events-calendar/2011/07/stolen-futures-forum-child-identity-theft>.



Data Security and Breach Notification Legislation: Selected Legal Issues

Alissa M. Dolan
Legislative Attorney

December 28, 2015

Congressional Research Service

7-5700

www.crs.gov

R44326

Summary

Recent data breaches at major U.S. retailers have placed a spotlight on concerns about the security of personal information stored in electronic form by corporations and other private entities. A data breach occurs when data containing sensitive personal information is lost, stolen, or accessed in an unauthorized manner, thereby causing a potential compromise of the confidentiality of the data. Existing federal laws, such as the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH Act), and the Gramm-Leach-Bliley Act, impose security and breach notification requirements on specific industries or types of data. Additionally, 47 states, the District of Columbia (D.C.), and three territories have enacted laws requiring breach notification, while at least 12 states have enacted data security laws, designed to reduce the likelihood of a data breach. Alabama, New Mexico, and South Dakota have not enacted breach notification laws.

Several data security and breach notification bills have been introduced in the 114th Congress, which broadly would impose security and notification requirements on businesses regardless of industry sector, with limited exceptions. This report begins by describing the common elements of these federal proposals and then discusses state laws that may apply in the event of a data breach.

The report then addresses two legal issues that may arise in consideration of new legislation about data security and breach notification. First, how would new federal legislation alter the application of existing state law or the availability of state law remedies for victims of data breaches? The report will discuss various forms of federal preemption (including express preemption, implied impossibility preemption, and implied obstacle preemption) and evaluate how a reviewing court might apply these preemption principles to federal proposals to determine which state laws would be superseded.

Second, the report examines the existing jurisdiction and enforcement authority of the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC) with regard to data security and breach notification requirements. This section analyzes the FTC's unfair or deceptive acts and practices authority under the Federal Trade Commission Act and the FCC's authority to regulate data security and breach notification for common carriers and cable and satellite providers under the Communications Act. Finally, it evaluates how the current federal proposals would change the enforcement responsibilities of each agency, potentially increasing the jurisdiction of the FTC and limiting the FCC's ability to enforce its existing data security rules.

Contents

Introduction	1
Proposed Legislation on Data Security and Breach Notification	2
State Laws Pertaining to Data Security and Breach Notification.....	3
Preemption of State Laws, Regulations, and Claims.....	4
Express Preemption.....	5
Types of Actions Being Preempted.....	6
Subject Matter of Preempted Actions	9
Implied Conflict Preemption.....	12
Impossibility Preemption	12
Obstacle Preemption	13
Agency Enforcement of Data Security and Breach Notification Requirements	15
Current FTC Authority: Unfair or Deceptive Acts and Practices.....	15
Current FCC Authority.....	16
Common Carriers.....	17
Cable and Satellite Providers	19
Proposed Changes to FTC and FCC Enforcement Authority.....	19

Contacts

Author Contact Information	21
----------------------------------	----

Introduction

Recent data breaches at major U.S. retailers have placed a spotlight on concerns about the security of personal information stored in electronic form by corporations and other private entities. A data breach occurs when data containing sensitive personal information is lost, stolen, or accessed in an unauthorized manner, thereby causing a potential compromise of the confidentiality of the data. Existing federal law imposes security and breach notification requirements on specific industries or types of data. For example, certain health information is subject to requirements under the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH Act), while certain financial institutions are subject to requirements under the Gramm-Leach-Bliley Act (GLB).¹ Additionally, 47 states, the District of Columbia (D.C.), and three territories have enacted laws requiring breach notification,² while at least 12 states have enacted data security laws.³

Several data security and breach notification bills have been introduced in the 114th Congress, which broadly would impose security and notification requirements on businesses regardless of industry sector, with limited exceptions. Many of the current proposals would leave existing federal requirements in place and exempt institutions and/or data covered by those federal laws from a new regulatory scheme. However, some bills would also propose to supersede existing state laws and prevent states from acting in this area, thereby creating a uniform federal standard throughout the country.

During consideration of proposed bills, two prominent legal issues have arisen. First, to what extent would federal legislation preempt state and local actions (including statutes, regulations, and/or the ability to bring legal claims) regarding data security and breach notification? Second, what effect would such legislation have on the existing authority of the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC) to bring enforcement actions related to data security and breach notification?

This report will discuss these two issues, starting with an examination of the Supreme Court's precedent regarding federal preemption. It will then analyze how these preemption principles might be applied by a reviewing court seeking to determine the preemptive effect of different federal proposals. Next, it will examine the existing jurisdiction and enforcement authority of the FTC and the FCC with regard to data security and breach notification as applied to telecommunications providers and how these agencies' responsibilities might be altered by proposed legislation.

¹ The Federal Information Security Management Act (FISMA) establishes standards for security and breach notification for information stored by federal agencies. P.L. 107-347, Title II, as amended by P.L. 113-283, *codified at* 44 U.S.C. §§ 3551, et seq. This report does not discuss requirements and considerations related to federal agency data.

² For a list of all state and territory statute citations, see National Conference of State Legislatures, "Security Breach Notification Laws," <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>. As of October 22, 2015, Alabama, New Mexico, and South Dakota do not have data breach notification laws.

³ See *infra* note 17.

Proposed Legislation on Data Security and Breach Notification

Several bills relating to data security and breach notification have been introduced in the 114th Congress.⁴ The bills take different approaches to imposing data security requirements on covered entities, if at all. For example, some bills establish specific criteria required for a covered entity's data security program, including elements such as design, risk assessment and management, and employee training.⁵ Other bills empower the FTC to write rules regarding data security, and require the FTC to address certain topics in those rules.⁶ Still others simply state that covered entities must employ reasonable security measures and practices, without identifying what those measures and practices must be.⁷ In general, a violation of the data security requirements or standards would be considered to be an unfair or deceptive act or practice, enforceable by the FTC.

Regarding notification, generally, a covered entity is required to provide notice when personal information contained in electronic data that it owns or possesses is either (1) accessed *or* acquired or (2) accessed *and* acquired, without authorization. Each bill defines what entities are covered and what constitutes personal information. Notification must usually be provided to residents and/or citizens of the United States as well as to the FTC and, in some cases, credit reporting agencies. Each bill establishes a deadline for notification, either within a certain number of days (such as 30 or 45 days) or as "expediently as possible and without unreasonable delay" after discovering the breach. Delayed notification is required if notice would jeopardize certain kinds of law enforcement investigations or national security.

Each bill defines the required form of notification, which may include written notice by mail or notice by email, when certain conditions are met. In certain circumstances, substitute notification through a posting on a website or publication may be an acceptable replacement for individual notification. The content of the notification includes such elements as the kind of personal information that has been breached, a phone number to contact for further information, and, potentially, information about the availability of free credit reporting services. However, in most cases, if the covered entity determines that the breach poses no reasonable risk of identity theft, fraud, or other unlawful conduct, then notification is not required. Notification requirements may also be waived if the entity is already required to provide notice under an existing federal law, such as HIPAA or GLB.

Violations of the notice requirements would typically be classified as unfair or deceptive acts or practices, which would be enforced by the FTC under existing regulations. Some bills would specifically empower the FTC to write regulations to implement the notification requirements, while others would not.⁸ Along with enforcement by the FTC, some of the proposals allow state

⁴ This report will reference the following bills: H.R. 580, the Data Accountability and Trust Act; H.R. 1053 and S. 547, the Commercial Privacy Bill of Rights Act of 2015; H.R. 1704, the Personal Data Notification and Protection Act; H.R. 1770, the Data Security and Breach Notification Act of 2015; H.R. 2205 and S. 961, the Data Security Act of 2015; S. 177, the Data Security and Breach Notification Act of 2015; S. 1027, the Data Breach Notification and Punishing Cyber Criminals Act of 2015; and S. 1158, the Consumer Privacy Protection Act of 2015.

⁵ *See, e.g.*, S. 1158, § 202.

⁶ *See, e.g.*, H.R. 580, § 2(a).

⁷ *See, e.g.*, H.R. 1770, § 2.

⁸ *See, e.g.*, H.R. 580, § 3(i) (granting the FTC authority to promulgate regulations to "effectively enforce" the bill's notification requirements); H.R. 1770 (providing no specific grant of rulemaking authority to the FTC).

attorneys general to enforce violations of the rules that affect people in their state through the filing of civil actions.⁹

Some bills contain additional provisions that go beyond security and breach notification and address topics such as data privacy.¹⁰ Additionally, as discussed further below, some bills specifically address the treatment of telecommunications common carriers, while others are silent on the subject. The details of each bill differ and close inspection of each provision and definition is required to determine its specific effect.

State Laws Pertaining to Data Security and Breach Notification

Forty-seven states, D.C., Guam, Puerto Rico, and the U.S. Virgin Islands have enacted legislation requiring businesses to notify affected persons when a data breach occurs.¹¹ For example, California law requires that businesses that own or license computerized data that include personal information provide notice of a data breach to residents of California in the “most expedient time possible and without unreasonable delay.”¹² A breach occurs when such unencrypted data is “acquired by an unauthorized person.”¹³ The required notice may be delayed if a law enforcement agency determines that the notice “will impede a criminal investigation.”¹⁴ The notice must be written in plain language and provide specific information: the name and contact information of the reporting entity; the type of personal information involved in the breach; the approximate date of the breach, if known; a general description of the “breach incident”; and, in certain circumstances, information about credit reporting agencies and identity theft prevention.¹⁵ In addition to notifying individuals whose information is acquired, if the breach affects more than 500 California residents, the entity must also notify the state attorney general.¹⁶

At least 12 states also have laws specifically addressing data security.¹⁷ For example, Massachusetts has promulgated regulations requiring persons who own or license personal information about a Massachusetts resident to “develop, implement, and maintain a

⁹ See, e.g., H.R. 1704, § 108; S. 177, § 5(d).

¹⁰ See, e.g., H.R. 1053.

¹¹ For a list of all state and territory statute citations, see National Conference of State Legislatures, “Security Breach Notification Laws,” <http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx>. As of October 22, 2015, Alabama, New Mexico, and South Dakota do not have data breach notification laws.

¹² CAL. CIV. CODE § 1798.82(a).

¹³ *Id.*

¹⁴ *Id.* at § 1798.82(c).

¹⁵ *Id.* at § 1798.82(d).

¹⁶ *Id.* at § 1798.82(f).

¹⁷ Arkansas (ARK. CODE § 4-110-104); California (CAL. CIV. CODE § 1798.81.5); Connecticut (Conn. Pub. Acts No. 08-167); Florida (FLA. STAT. §§ 282.318, 501.171); Indiana (IND. CODE § 24-4.9-3-3.5); Maryland (MD. CODE ANN., COM. LAW § 14-3501); Massachusetts (201 MASS. CODE REGS. § 17.00) (issued pursuant to MASS. GEN. LAWS ch. 93H); Nevada (NEV. REV. STAT. § 603A.210); Oregon (OR. REV. STAT. § 646A.622); Rhode Island (R.I. GEN. LAWS § 11-49.2); Texas (TEX. BUS. & COM. CODE § 48.102); Utah (UTAH CODE § 13-44-201). Other state laws may impose data protection requirements on information held by the state government. For example, Montana recently enacted a law requiring state agencies that maintain personal information to develop procedures to protect that data. H.B. 123, § 26 (2015).

comprehensive information security program....”¹⁸ Such a program must be in writing and contain administrative, technical, and physical safeguards that are appropriate based on the size and type of business, available resources, and the amount of stored data.¹⁹ Every program shall complete specific tasks, such as “identifying and assessing reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity” of data; developing employee security policies on storage, access, and transportation of records; and regularly monitoring the program to ensure that it is “operating in a manner reasonably calculated to prevent unauthorized access” to data.²⁰ Businesses must also conduct an annual review of security measures.²¹

Finally, states may have general consumer protection laws that could potentially be used to remedy the harm caused by a data breach. For example, Illinois law makes unlawful “unfair methods of competition and unfair or deceptive acts or practices ... in the conduct of any trade or commerce.”²² This law includes prohibitions on “deception fraud, false pretense, false promise, misrepresentation or the concealment, suppression, or omission of any material fact, with intent that others rely upon the concealment....”²³ Individuals whose personal information is compromised in a data breach may attempt to use such a consumer protection law to allege that the breached entity’s failure to disclose its inadequate security measures amounts to an unfair or deceptive practice in violation of state law.²⁴

Preemption of State Laws, Regulations, and Claims

A major question related to consideration of federal legislation addressing data security and breach notification is whether, and to what extent, the federal law should preempt these existing state laws, thereby displacing state-by-state requirements in favor of a uniform, federal standard for entities covered under the general requirements established in the proposed legislation discussed above.

Federal preemption is rooted in the Supremacy Clause of the U.S. Constitution, which states that “[t]he Constitution, and the Laws of the United States which shall be made in Pursuance thereof; and all Treaties made, or which shall be made, under the Authority of the United States, shall be the supreme Law of the Land.”²⁵ Under the Supremacy Clause, Congress can override any state and local law that falls within Congress’s legislative authority.²⁶ Therefore, the legal issue is not whether Congress has the ability to preempt state and local laws but rather determining the

¹⁸ 201 MASS. CODE REGS. 17.03(1).

¹⁹ *Id.*

²⁰ *Id.* at 17.03(2).

²¹ *Id.* at 17.03(2)(i).

²² 815 ILL. COMP. STAT. 505/2.

²³ *Id.*

²⁴ It may be difficult for plaintiffs to prevail on claims brought under a state general consumer protection statute due to the specific elements that must be proven in order to succeed on such a claim. *See, e.g., In re Michaels Stores Pin Pad Litig.*, 830 F. Supp. 2d 518 (N.D. Ill. 2011) (concluding that the plaintiffs failed to allege a deceptive practice under the Illinois Consumer Fraud and Deceptive Business Practices Act because plaintiffs could not identify any communications by Michaels, the subject of the data breach, containing the allegedly deceptive omission—that it did not implement adequate security measures). Required elements may differ in each state’s law.

²⁵ U.S. CONST. art. IV, cl. 2.

²⁶ *Crosby v. Nat’l Foreign Trade Council*, 530 U.S. 363, 372 (2000) (“A fundamental principle of the Constitution is that Congress has the power to preempt state law.”).

particular circumstances under which federal law, either explicitly or implicitly, preempts state and local laws.

In answering the question of when preemption occurs, the Supreme Court has at times emphasized “two cornerstones of [] pre-emption jurisprudence.”²⁷ First, “the purpose of Congress is the ultimate touchstone in every pre-emption case.”²⁸ Second, “[i]n all pre-emption cases, and particularly in those in which Congress has ‘legislated ... in a field which the States have traditionally occupied,’ we ‘start with the assumption that the historic police powers of the States were not to be superseded by the Federal Act unless that was the clear and manifest purpose of Congress.’”²⁹ There are two kinds of federal preemption: express preemption and implied preemption.³⁰

Express Preemption

Express preemption occurs when a federal statute explicitly states its intent to preempt state and/or local action on a given subject. By including such language, Congress expresses its clear intent that the federal statute is to supersede state attempts to regulate on the issue. If a federal law is deemed to preempt a state law, regulation, or cause of action, then the preempted state law, regulation, or cause of action cannot be the basis for enforcement against covered entities.

Congress may also choose to include a “saving clause” in addition to an express preemption clause. A saving clause seeks to preserve some role for state or local action, by “saving” certain actions from the scope of the express preemption clause. Where a saving clause is present, the express preemption clause and saving clause must be read together in order to determine what kinds of actions will ultimately be superseded under express preemption principles.³¹

All of the current federal legislative proposals in the area include express preemption clauses. Each express preemption clause typically raises at least two different issues: first, the *types* of

²⁷ *Wyeth v. Levine*, 555 U.S. 555, 565 (2009).

²⁸ *Medtronic, Inc. v. Lohr*, 518 U.S. 470, 485 (1996).

²⁹ *Id.* (quoting *Rice v. Santa Fe Elevator Corp.*, 331 U.S. 218, 230 (1947)). Some commentators have noted that the presumption against preemption has not been uniformly applied in recent Supreme Court cases. *See, e.g.*, Ernest A. Young, “*The Ordinary Diet of the Law*”: *The Presumption Against Preemption in the Roberts Court*, 2011 SUP. CT. REV. 253, 307 (2011) (“In theory, at least, the centerpiece of modern preemption doctrine remains the Court’s statement in *Rice v. Santa Fe Elevator Corp.* that ‘we start with the assumption that the historic police powers of the States were not to be superseded by the Federal Act unless that was the clear and manifest purpose of Congress.’ Just three years ago, in *Wyeth*, the Court described the *Rice* presumption as a ‘cornerstone[] of our pre-emption jurisprudence.’ Notwithstanding this and similar endorsements, many scholars have noted the Court’s failure to consistently employ the *Rice* canon. The 2010 Term was no exception to this tendency: The Justices ignored *Rice* in *Williamson* and *Concepcion* and invoked it only in dissent in *PLIVA* and *Bruesewitz*. In *Whiting*, the majority looked only to the ‘plain wording’ of the express preemption clause, but imposed a ‘high threshold’ for finding conflict preemption.”); Thomas W. Merrill, *Symposium: Ordering State-Federal Relations Through Federal Preemption Doctrine: Preemption and Institutional Choice*, 102 NW. U.L. REV. 727, 741-43 (2008); Mary J. Davis, *Unmasking the Presumption in Favor of Preemption*, 53 S.C. L. REV. 967 (2002).

³⁰ Implied preemption can be further broken down into two categories, field preemption and conflict preemption, discussed below. *See* “Implied Conflict Preemption.”

³¹ *Geier v. American Honda Motor Co.*, 529 U.S. 861, 868 (2000). In *Geier*, the Supreme Court held that the preemption and saving clauses of the National Traffic and Motor Vehicle Safety Act of 1966 had to be read together such that the text of both clauses is given “actual meaning.” *Id.* *See also* *Sprietsma v. Mercury Marine*, 537 U.S. 51 (2002).

state and local actions³² intended to be displaced and second, the *subject matter* of the preempted actions. For example, the express preemption clause in H.R. 1770 states:

No State or political subdivision of a State shall, with respect to a covered entity subject to this Act, adopt, maintain, enforce, or impose or continue in effect any law, rule, regulation, duty, requirement, standard, or other provision having the force and effect of law relating to or with respect to the security of data in electronic form or notification following a security breach of such data.³³

The type of state and local actions covered by this clause would be “any law, rule, regulation, duty, requirement, standard, or other provision having the force and effect of law...”³⁴ The subject matter of the preempted actions would be those “relating to or with respect to the security of data in electronic form or notification following a security breach of such data.”³⁵ Therefore, if a state action is of the type covered by the clause, falls within the subject matter of the clause, and is adopted, maintained, enforced, or imposed or continued in effect by the state, the action will be expressly preempted under this clause.

When evaluating express preemption clauses, courts rely on principles of statutory interpretation to determine if a given state or local action is preempted. In trying to effectuate congressional intent, courts look to the “language of the pre-emption statute and the ‘statutory framework’ surrounding it”³⁶ as well as the “structure and purpose of the statute as a whole.”³⁷ Therefore, analyzing an express preemption clause is a context-driven exercise, where the specific words in the statute and the intent of the legislative scheme as a whole are of crucial importance.

Types of Actions Being Preempted

Congress can choose to displace any state or local action in an express preemption clause. State actions subject to federal preemption could include positive law enactments, such as state statutes and regulations. State common law, such as the ability to bring lawsuits under theories including breach of contract, negligence, or other torts, can also be preempted by federal law. Both positive law enactments and state common law claims will be referred to as “state actions” throughout this report.

Positive Law

All of the express preemption clauses in the proposed federal data security and breach notification bills are likely to be interpreted as preempting state positive law enactments governing the specific subject matter. Express preemption clauses that use words such as “law,” “statute,” and/or “regulation” would preempt positive enactments of state and local law. Additionally, positive law enactments clearly impose “requirements” or “prohibitions”³⁸ and, therefore, clauses using those phrases will also have the effect of preempting state positive law.

³² State and local actions could include the enactment of state statutes, promulgation of regulations, and the ability to bring legal claims under state common law.

³³ H.R. 1770, § 6(a).

³⁴ *Id.*

³⁵ *Id.*

³⁶ *Medtronic*, 518 U.S. at 486 (quoting *Gade v. National Solid Wastes Management Ass’n*, 505 U.S. 88, 111 (1992) (Kennedy, J., concurring in part and concurring in judgment)).

³⁷ *Id.* (quoting *Gade*, 505 U.S. at 98).

³⁸ See *Cipollone v. Liggett Group*, 505 U.S. 504, 521 (1992).

Common Law Causes of Action

Less clear is which of the proposed bills are likely to be interpreted as also preempting common law causes of action.³⁹ The Court has ruled that express preemption clauses referring to “requirements,” “standards,” or “other provisions with the force or effect of law” cover duties imposed by common law and, therefore, could preempt common law causes of action.⁴⁰ For example, in *Cipollone v. Liggett Group*, a plurality of the Supreme Court held that a provision preempting a state-imposed “requirement or prohibition based on smoking and health” “plainly reaches beyond [positive] enactments” and “easily encompass[es] obligations that take the form of common-law rules....” since the common law actions at issue were premised on the existence of a legal duty.⁴¹ Furthermore, the Court’s precedent indicates that the word “rule” in the phrase “any provision of statute, rule, or regulation” arguably encompasses common law claims.⁴² In *Sprietsma*, the Court noted that if one interpreted the word “law” in the phrase “law or regulation” (as used in the express preemption clause) to encompass both positive law enactments and common law rules, then the term “regulation” becomes superfluous.⁴³ Similarly, here, one could argue that if one interprets “statute, regulation, or rule” as encompassing only positive law enactments, then the use of the word “rule” is superfluous. Therefore, the better interpretation of the phrase, that gives meaning to each of the words contained therein, appears to be one that encompasses both positive law enactments and common law rules. Therefore, bills that use this wording likely would preempt common law causes of action.

Bills preempting “any provision of the law of any state” may also be interpreted to include common law claims within the scope of express preemption.⁴⁴ The Court has noted that “[i]t is routine to call common law rules ‘provisions’”⁴⁵ and federal courts have previously treated

³⁹ See, e.g., H.R. 580, § 6(a) (“This Act supersedes any provision of a statute, regulation, or rule of a State ...”); H.R. 1770, § 6(a) (“No State or political subdivision of a State shall, with respect to a covered entity subject to this Act, adopt, maintain, enforce, or impose or continue in effect any law, rule, regulation, duty, requirement, standard, or other provision having the force and effect of law ...”); H.R. 2205, § 6 (“No requirement or prohibition may be imposed under the laws of any State ...”); S. 177, § 7(a) (“[T]his Act supersedes any provision of a statute, regulation, or rule of a State ...”); S. 961, § 6 (“No requirement or prohibition may be imposed under the laws of any State ...”); S. 1027, § 8 (“This Act preempts any law, rule, regulation, requirement, standard, or other provision having the force and effect of law of any State ...”).

⁴⁰ *Cipollone*, 505 U.S. at 521 (determining that the term “requirement or prohibition” encompasses common law obligations); see also *Bates v. Dow Agrosciences*, 544 U.S. 431, 443 (2005) (concluding that the term “requirement” in the express preemption clause of the Federal Insecticide, Fungicide, and Rodenticide Act “reaches beyond positive enactments, such as statutes and regulations, to embrace common-law duties”); *Northwest, Inc. v. Ginsberg*, 134 S. Ct. 1422 (2014) (declaring that state common law rules fall comfortably within a provision preempting a state “law, regulation, or other provision having the force and effect of law ...”); *CSX Transp. v. Easterwood*, 507 U.S. 658, 664 (1993) (finding that legal duties imposed by common law fall within the scope of a clause preempting any state “law, rule, regulation, order, or standard relating to railroad safety”).

⁴¹ *Cipollone*, 505 U.S. at 521.

⁴² The Supreme Court frequently refers to common-law claims and obligations as “rules.” See, e.g., *Ginsberg*, 134 S. Ct. at 1429-30; *Altria Group, Inc. v. Good*, 555 U.S. 70, 81 (2008); *CSX Transp.*, 507 U.S. at 675; *Cipollone*, 505 U.S. at 521-22.

⁴³ *Sprietsma*, 537 U.S. at 63.

⁴⁴ See, e.g., H.R. 1053, § 156 (“The provisions of this title shall supersede any provisions of the law of any State....”); H.R. 1704, § 109 (“The provisions of this title shall supersede any provision of the law of any State....”); S. 547, § 156 (“The provisions of this title shall supersede any provisions of the law of any State....”); S. 1158, § 220 (“[T]he provisions of this subtitle shall supersede... any provisions of the law of any State....”).

⁴⁵ *Ginsberg*, 134 S. Ct. at 1429 (citing *Madsen v. Women’s Health Center, Inc.*, 512 U.S. 753, 765 (1994); *United States v. Barnett*, 376 U.S. 681, 689-700 (1964); *Brown v. United Airlines, Inc.*, 720 F.3d 60, 68 (1st Cir. 2013)). Additionally, the Supreme Court has suggested that the use of the term “law” alone in an express preemption clause (continued...)

common law claims as the type of claim that could be preempted in statutes that supersede “any provision of state law.”⁴⁶ While this appears to be the best interpretation of this type of bill, the case law does not provide clear answers. It is likely that both the continued viability of the presumption against preemption⁴⁷ and the text and purpose of the broader statutory scheme would have to be closely considered before deciding the appropriate interpretation of these clauses.⁴⁸

If common law actions are eligible for preemption under an express preemption clause, a reviewing court must still determine if the specific action being brought satisfies all elements of the clause. Not all common law actions may be considered to be laws of the state or laws imposed by the state. For example, on several occasions, the Supreme Court has drawn a distinction between common law claims that seek to enforce obligations imposed by the state and claims that derive from self-imposed obligations, voluntarily undertaken by the parties. In *American Airlines v. Wolens*, the Court concluded that although some common law claims could be preempted under the express preemption clause at issue, a breach of contract claim would not be superseded because the contract represented “privately ordered obligations,” not provisions that were enacted or enforced by the state.⁴⁹ Therefore, a common law claim that seeks to enforce self-imposed

(...continued)

may lead to a different meaning than if the clause applied to both “law” and “regulation.” See *Sprietsma*, 537 U.S. at 63 (nothing that “‘a word is known by the company it keeps’” and, therefore, “the terms ‘law’ and ‘regulation’ used together in the pre-emption clause indicated that Congress pre-empted only positive enactments. If ‘law’ were read broadly so as to include the common law [when used in conjunction with regulation], it might also be interpreted to include regulations, which would render the express reference to ‘regulation’ in the pre-emption clause superfluous.” (internal citations omitted)).

⁴⁶ In evaluating the express preemption clause of the Expedited Funds Availability Act (EFAA), which states that the EFAA “shall supersede any provision of the law of any State... which is inconsistent with this chapter,” the U.S. Court of Appeals for the Ninth Circuit concluded that the plaintiff’s common law claims were not preempted. *Beffa v. Bank of the West*, 152 F.3d 1174 (9th Cir. 1998). The court did not hold that the text of the EFAA clause applied only to positive law enactments and not common law claims. Instead, the court appeared to assume that the EFAA provision could preempt a common law claim if it fell within the subject matter of the clause and was inconsistent with the EFAA. In this case, the court simply determined that the claims being brought were outside the scope of the subject matter of the clause. *Id.* at 1177. See also *Aresty Int’l Law Firm, P.C. v. Citibank, N.A.*, 677 F.3d 54 (1st Cir. 2012) (interpreting the EFAA express preemption clause and evaluating whether a common law claim fell within the subject matter of the clause). The U.S. Court of Appeals for the Second Circuit, in evaluating the effect of the Federal Election Campaign Act’s (FECA) express preemption clause, undertook a similar analysis. *Stern v. General Electric, Co.*, 924 F.2d 472 (2d Cir. 1991). That clause applies to “any provision of State law with respect to election to Federal office.” 52 U.S.C. § 30143. The court found that the plaintiff’s shareholder derivative suit was not preempted by FECA, not because the claims were not the *type* of claim that fell within the meaning of the clause, but because the claims were not within the subject matter of the clause. *Stern*, 924 F.2d at 475.

In non-preemption contexts, the Court has also interpreted the phrase “state law” to include both positive law enactments and common law claims. See *Cipollone*, 505 U.S. at 522; *Norfolk & Western R. Co. v. Train Dispatchers*, 499 U.S. 117, 128 (1991) (concluding that a federal law providing rail carriers with exemptions from “all other law, including state and municipal law” “does not admit of [a] distinction... between positive enactments and common-law rules of liability”).

⁴⁷ See *supra* note 29 and accompanying text.

⁴⁸ One could argue, as the *Cipollone* Court noted, that even if “state law” has been interpreted broadly in other contexts so as to encompass common law claims, the presumption against preemption should counsel against such an interpretation in an express preemption context. *Cipollone*, 505 U.S. at 504 (“Although the presumption against preemption might give good reason to construe the phrase ‘state law’ in a pre-emption provision more narrowly than an identical phrase in another context, in this case such a construction is not appropriate.”).

⁴⁹ *Am. Airlines v. Wolens*, 513 U.S. 219, 228 (1995); see also *Ginsberg*, 134 S. Ct. at 1431-33 (noting that whether a breach of implied covenant of good faith and fair dealing claim was preempted depended upon whether a state allowed parties to contract out of the covenant.).

obligations would likely not be considered a rule or standard enacted or enforced by the state and is unlikely to be preempted under these types of express preemption clauses.

A reviewing court may also need to delve into the elements of the common law action to determine if it satisfies all of the elements of an express preemption clause. For example, in *Bates v. Dow Agrosciences*, the Supreme Court concluded that an express warranty claim regarding a pesticide label was not preempted by a provision applying to “requirements for labeling or packaging.”⁵⁰ The common law rule underlying the express warranty claim did not require the manufacturer to make an express warranty, it only required that the manufacturer “make good” on the commitment it voluntarily undertook. Therefore, even though losing such a claim would likely induce the manufacturer to change its label, the claim itself still did not constitute a requirement as contemplated by the preemption provision.⁵¹

Saving Clauses

As noted above, if a saving clause is present, it must be read in conjunction with an express preemption clause to determine what types of state actions will ultimately be superseded based on express preemption.

For example, an express preemption clause that preempts “any law, rule, regulation, duty, requirement, standard, or provision having the force and effect of law” would likely be interpreted as preempting state statutes, regulations, and common law causes of action. However, if that bill has a saving clause stating that the express preemption clause “shall not exempt a covered entity from liability under common law,” the express preemption analysis changes.⁵² Reading the express preemption and saving clauses together, it is likely that such a bill would be interpreted as expressly preempting state positive law enactments but not state common law causes of action. Saving clauses may also identify specific kinds of laws that are not to be preempted. For example, a saving clause may shield “state trespass, contract, or tort law” from express preemption.⁵³

Ultimately, the existence of a saving clause can significantly change the scope of an express preemption clause and must be read in light of the plain text, express preemption clause, and the purpose of the statute as a whole.⁵⁴

Subject Matter of Preempted Actions

Existing federal proposals vary in defining the subject matter of state actions to be preempted. Some bills define the subject matter of preempted actions narrowly, by preempting state statutes, regulations, and/or common law claims that “require” or “expressly require” certain actions.⁵⁵ For example, H.R. 580 preempts a state action that

expressly—

- (1) requires information security practices and treatment of data containing personal information similar to any of those required under section 2; and

⁵⁰ *Bates v. Dow Agrosciences*, 544 U.S. 431, 443-46 (2005).

⁵¹ *Id.* at 445.

⁵² See H.R. 1770, § 6(b).

⁵³ See, e.g., H.R. 580, § 6(c); S. 177, § 7(c).

⁵⁴ See *Geier*, 529 U.S. at 868.

⁵⁵ E.g., H.R. 580, § 6; S. 177, § 7; S. 1158, § 220.

(2) requires notification to individuals of a breach of security resulting in unauthorized access to or acquisition of data in electronic form containing personal information.⁵⁶

This clause is likely to expressly preempt only state laws, regulations, and common law causes of action⁵⁷ that specifically impose data security and breach notification requirements. It is unlikely that this kind of provision would be interpreted to preempt general state consumer protection statutes, since these statutes would not “expressly require” certain conduct with regard to security and notification, but rather impose general standards of behavior to be applied to all situations.

Alternatively, several bills use the term “relating to” when describing the subject matter of express preemption.⁵⁸ For example, S. 1027 preempts state actions “relating to the protection or security of data in electronic form containing personal information or the notification of a breach of security.”⁵⁹ Bills using the term “relating to” are likely to be interpreted as preempting a broader swath of state actions. The Supreme Court has described “relating to” within the context of express preemption clauses as broad and having an “expansive sweep.” In *Morales v. TWA*, the Court determined that a provision preempting actions “relating to rate, routes, or services of any air carrier” superseded not only state laws that directly addressed air carriers but laws of general applicability, such as a consumer protection statute, when applied to air carriers.⁶⁰ Later cases importantly noted that “the breadth of the words ‘related to’ does not mean the sky is the limit”⁶¹ and that such words should not be read “with an ‘uncritical literalism.’”⁶² For example, the Court has cautioned that an express preemption clause regarding motor carriers similar to the air carrier provision “does not preempt state laws affecting carrier prices, routes, or services ‘in only a tenuous, remote, or peripheral ... manner.’”⁶³

A bill that expressly preempts statutes and regulations “relating to” the protection or security of covered data or the notification of a breach of security⁶⁴ would clearly supersede state laws that directly address data security or notification, such as a statute establishing breach notification requirements. It would also likely preempt more general state laws, such as a consumer protection

⁵⁶ H.R. 580, § 6.

⁵⁷ This clause would only preempt common law causes of action that are not covered under the scope of its saving clause, which states: “This Act shall not be construed to preempt the applicability of—(1) State trespass, contract, or tort law; or (2) other State laws to the extent that those laws relate to acts of fraud.” H.R. 580, § 6(c).

⁵⁸ See, e.g., H.R. 1053, § 156; H.R. 1704, § 109; S. 547, § 156; S. 1027, § 8. Additionally, H.R. 1770 uses the term “relating to or with respect to.” H.R. 1770, § 6(a).

⁵⁹ S. 1027, § 8.

⁶⁰ *Morales v. TWA*, 504 U.S. 374, 383-84 (1992) (“The ordinary meaning of these words is a broad one—‘to stand in some relation; to have bearing or concern; to pertain; refer; to bring into association with or connection with,’—and the words thus express a broad pre-emptive purpose. We have repeatedly recognized that in addressing the similarly worded pre-emption provision of the Employee Retirement Income Security Act of 1974 (ERISA)... which pre-empts all state laws ‘insofar as they ... relate to any employee benefit plan.’ We have said, for example, that the ‘breadth of [that provision’s] pre-emptive reach is apparent from [its] language,’ ...; that it has a ‘broad scope,’ ... and an ‘expansive sweep,’ ...; and that it is ‘broadly worded,’ ... ‘deliberately expansive,’ ... and ‘conspicuous for its breadth’ ...”). See also *Wolens*, 573 U.S. at 228. The Court later described the *Wolens* decision by stating: “The plaintiffs in that case sought to bring a claim under the Illinois Consumer Fraud and Deceptive Business Practices Act. Our conclusion that the state-law claim was pre-empted turned on the unusual breadth of the ADA’s pre-emption provision, ‘relating to rates, routes, or services,’ is a broad one.” *Good*, 555 U.S. at 85.

⁶¹ *Dan’s City Used Cars, Inc. v. Pelkey*, 133 S. Ct. 1769, 1778 (2013).

⁶² *Id.* (quoting *N.Y. State Conference of Blue Cross & Blue Shield Plans v. Travelers Ins. Co.*, 514 U.S. 645, 655-56 (1995)).

⁶³ *Id.* (quoting *Rowe v. N.H. Motor Transp. Assn.*, 522 U.S. 364, 371 (2008)).

⁶⁴ E.g., S. 1027, § 8.

law that prohibits unfair and deceptive acts or practices, because such a law would “relate to” data security and notification when it is applied to a data breach.

Finally, some bills use the phrase “with respect to” to describe the subject matter of preempted state actions. For example, H.R. 2205 preempts state actions

with respect to the responsibilities of any person to—

- (1) protect the security of information relating to consumers that is maintained, communicated, or otherwise handled by, or on behalf of, the person;
- (2) safeguard information relating to consumers from—
 - (A) unauthorized access; and
 - (B) unauthorized acquisition;
- (3) investigate or provide notice of the unauthorized acquisition of, or access to, information relating to consumers, or the potential misuse of the information, for fraudulent, illegal, or other purposes; or
- (4) mitigate any potential or actual loss or harm resulting from the unauthorized acquisition of, or access to, information relating to consumers.⁶⁵

The courts have provided less guidance on the meaning of this phrase and it is unclear if the phrase is likely to be interpreted as similar to “relating to” or narrower in scope. Federal courts have considered at least one express preemption clause that uses “with respect to.” The clause, from the Federal Election Campaign Act (FECA), preempted “any provision of state law with respect to election to federal office”⁶⁶ and has been interpreted relatively narrowly. The U.S. Court of Appeals for the Fifth Circuit found that the act did not preempt a claim based on a general state fraud statute. In reaching this conclusion, the court appeared to draw a distinction between statutes that specifically regulated federal elections, which would be preempted, and statutes of general applicability that could be applied to federal election activities, which would not be preempted.⁶⁷ However, it is unclear if the court’s analysis was based strictly on a plain language interpretation or if it relied equally on the text and purpose of the overall legislative scheme.

If a federal law that preempted state statutes and regulations “with respect to” data security were interpreted narrowly, like the FECA provision, it likely would preempt state laws that establish data security standards, but would not preempt a general consumer protection statute. Alternatively, if the provision were interpreted more broadly, it could encompass both the direct data security laws as well as laws of general applicability, such as general consumer protection laws. In this instance, the statute’s underlying congressional intent may help guide a court’s interpretation of an arguably ambiguous express preemption clause.

⁶⁵ H.R. 2205, § 6. *See also* S. 961, § 6. Additionally, H.R. 1770 uses the term “relating to or with respect to.” H.R. 1770, § 6(a).

⁶⁶ 52 U.S.C. § 30143.

⁶⁷ *Janvey v. Democratic Senatorial Campaign Comm., Inc.*, 712 F.3d 185, 200-01 (5th Cir. 2013). Additionally, the U.S. Court of Appeals for the Second Circuit described the clause as containing “narrow wording” that “suggests that Congress did not intend to preempt state regulation with respect to non-election-related activities.” *Stern*, 924 F.2d at 475.

Implied Conflict Preemption

The existence of an express preemption provision and/or a saving clause would not necessarily settle the question of the scope of potential preemption under a federal data security and breach notification statute. The Supreme Court has “made clear that the existence of a separate [express] pre-emption provision ‘does not bar the ordinary working of conflict pre-emption principles.’”⁶⁸ Therefore, after determining the scope of express preemption, a reviewing court may then need to determine if state actions that would not be expressly preempted may, nonetheless, be preempted under principles of implied conflict preemption.⁶⁹

Conflict preemption can be present in two instances: first, where compliance with both the state and federal law is a physical impossibility (impossibility preemption)⁷⁰ and second, when the state action “stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress”⁷¹ (obstacle preemption).

Impossibility Preemption

Impossibility preemption has previously been described by the Supreme Court as a situation in which a state law prohibits what the federal law requires, or vice versa.⁷² Generally, it requires the presence of conflicting affirmative legal obligations imposed by state and federal law. For example, the Supreme Court provided a useful illustration of these principles in *Florida Lime & Avocado Growers v. Paul*.⁷³ In a hypothetical it constructed, the Court noted that a state law preventing the picking and marketing of avocados testing less than 8% of oil would be preempted under impossibility preemption if a federal law forbade the picking and marketing of avocados testing more than 7% oil.⁷⁴

However, where a state or federal law simply permits an activity the other restricts or prohibits, impossibility preemption appears not to apply.⁷⁵ Commentators have suggested that instances of impossibility preemption are relatively rare.⁷⁶

⁶⁸ *Hillman v. Maretta*, 133 S. Ct. 1943, 1954 (2013) (citing *Sprietsma*, 537 U.S. at 65).

⁶⁹ Implied preemption can also occur when a “scheme of federal regulation is so pervasive as to make reasonable the inference that Congress left no room for the states to supplement it.” *Rice*, 331 U.S. at 230. This type of implied preemption is called field preemption, because Congress has occupied the field within the given subject area such that states may not regulate. This type of preemption is not addressed in this report.

⁷⁰ *Florida Lime & Avocado Growers v. Paul*, 373 U.S. 132, 142-43 (1963).

⁷¹ *Hines v. Davidowitz*, 312 U.S. 52, 67 (1941).

⁷² The Court has noted that impossibility preemption is a “demanding defense.” *Wyeth*, 555 U.S. at 573.

⁷³ *Paul*, 373 U.S. at 143.

⁷⁴ *Id.*

⁷⁵ See *Wyeth*, 555 U.S. at 571-72 (finding that impossibility preemption did not exist because state law required the drug manufacturer to add an adequate warning about the risk of IV-push administration and that federal law permitted the manufacturer to make such a label change before the FDA approved it); *Barnett Bank v. Nelson*, 517 U.S. 25, 31 (1996) (noting that the two statutes at issues in the case “do not impose directly conflicting duties on national banks—as they would, for example, if the federal law said, ‘you must sell insurance,’ while the state law said, ‘you may not’”). In *Mutual Pharmaceutical Company v. Bartlett*, the Supreme Court held that a state tort defective design claim against a generic drug manufacturer was preempted by federal law due to impossibility preemption. *Mutual Pharm. Co. v. Bartlett*, 133 S. Ct. 2466 (2013). The Court concluded that the state common law required the manufacturer to strengthen the warnings on the drug’s label. *Id.* at 2475. However, the manufacturer was prohibited under federal law from changing the label. *Id.* at 2476. Therefore, since the state law required action that the federal law prohibited, compliance with both was impossible. *Id.* at 2477. The Court rejected the lower court’s finding that impossibility preemption should not apply because the drug manufacturer could choose to stop selling the drug altogether. If such a (continued...)

To illustrate the application of impossibility preemption, consider a hypothetical federal law that expressly preempts less stringent state data breach notification laws, thereby setting a floor for minimum protection but allowing states to impose stricter standards.⁷⁷ The federal standard requires covered entities to notify affected persons as expediently as possible and generally within 30 days of discovering a breach, but also provides exceptions under which notification would be delayed, for example if it would impede a criminal investigation or for national security reasons.⁷⁸ A state data breach notification statute that imposed more stringent requirements than the federal law would survive under an express preemption analysis but could still be superseded due to impossibility preemption. Under the state statute, a covered entity must delay notification to the affected parties if it would impede a criminal or civil investigation.⁷⁹ Assume a covered entity experiences a data breach that triggers both state and federal notification requirements and that notification of that breach would impede a civil investigation. Under the state statute described, the covered entity would be prohibited from providing notice to the affected parties until cleared by law enforcement. However, under the federal law described, which does not allow for delayed notification because of an ongoing civil investigation, the entity would be required to provide notice within 30 days. Since the federal law requires the entity to take action that is prohibited under state law, compliance with both laws would be impossible. Therefore, a reviewing court is likely to conclude that the state law is preempted under impossibility preemption.

Obstacle Preemption

Obstacle preemption analysis is broader in scope. In determining when a state action “stands as an obstacle,” a reviewing court must consider congressional intent and the “purposes and objectives” of the federal statute as a whole.⁸⁰ “If the purpose of the act cannot otherwise be accomplished,” the Supreme Court has held, then “the state law must yield to the regulation of Congress....”⁸¹ Obstacle preemption can be difficult to apply, since it relies heavily on a reviewing court’s interpretation of Congress’s purposes in creating the legislative scheme at issue and may require a nuanced analysis of the applicable state law.

(...continued)

theory were accepted, the Court concluded that “impossibility preemption would be ‘all but meaningless.’” *Id.* Justice Sotomayor’s dissent disagreed with the majority’s reasoning because she found that the state common law did not create a requirement for the manufacturer to change the drug’s label. Instead, she characterized the tort action as creating an incentive for the manufacturer to take certain action to avoid future liability, but not an actual legal mandate. *Id.* at 2488-89 (Sotomayor, J., dissenting).

⁷⁶ Kerry Abrams, *Plenary Power Preemption*, 99 VA. L. REV. 601, 608-09 (2013).

⁷⁷ *E.g.*, S. 1158, § 220(a)-(b).

⁷⁸ *E.g.*, H.R. 1053, § 142(f); H.R. 1704, § 101(d); S. 1158, § 211(d).

⁷⁹ At least five state have data breach notification statutes that require delay of notification if it will jeopardize a civil investigation. *See, e.g.*, N.J. STAT. ANN. § 56:8-163(c)(2); OKLA. STAT. tit. 24, § 163(D); 73 PA. CONS. STAT. § 2304; VA. CODE ANN. § 18.2-186.6; W. VA. CODE § 46A-2A-102(e).

⁸⁰ *Crosby*, 530 U.S. at 373 (noting that in considering obstacle preemption, a court’s judgment is to be informed by “examining the federal statute as a whole and identifying its purpose and intended effects”).

⁸¹ *Id.* *Geier* provides an example of obstacle preemption when an express preemption clause is also present. In that case, the Supreme Court held that a plaintiff’s state tort claim, which was based on the theory that an automobile manufacturer had a duty under common law to install an airbag in its manufactured vehicles, was preempted. *Geier*, 529 U.S. at 874. Because the applicable federal law had the objective of ensuring a variety of passive restraint systems, just one of which was airbags, the state common law claim would have presented an obstacle to the accomplishment of this purpose. *Id.* at 881.

Consequently, proposals that focus on creating a uniform, nationwide standard for data security and breach notification⁸² are more likely to supersede state law under obstacle preemption—since the existence of individual state standards would prohibit national uniformity—than a federal law that instead focused on setting minimum national standards.

Determining whether a state common law cause of action that remains valid after an express preemption analysis would still be superseded under obstacle preemption can be particularly difficult. The outcome of such an analysis may depend upon how a reviewing court interprets the elements of the claim under state law and the precise purpose of the federal law. The Supreme Court confronted this kind of question regarding the nature of a state tort claim in *Mutual Pharmaceutical Company, Inc. v. Bartlett*.⁸³ In that case, the Court had to determine whether a New Hampshire tort design-defect claim was preempted by federal law under impossibility preemption. In discussing the specifics of the claim, the five Justices of the majority determined that the state tort cause of action imposed a duty on the defendant to take a specific remedial action and, therefore, was preempted.⁸⁴ However, two Justices writing in dissent argued that the state tort law did not impose an affirmative legal obligation on the defendant to take the remedial action. Instead, they stated that the claim “create[d] an incentive” for the defendant or similar entities to make changes to their products “to try to avoid liability.”⁸⁵ This case highlights the complexity of this analysis, which depends on a court’s interpretation of the specific elements of the state common law claim, and the possibility that judges may come to differing conclusions about the proper analysis of a specific claim.

Similarly, a reviewing court could view a negligence claim, if successful, as creating a legal duty for the defendant to implement better data security practices, including potentially a specific type of security mechanism. Under this view, the defendant and similarly situated entities in that state would then be subject to a legal requirement imposed by state common law to adopt those security practices, which a review court may determine to be in conflict with a federal law whose purpose is to create one uniform standard nationwide. Alternatively, a reviewing court might view that common law negligence claim as simply a request by the plaintiffs to be compensated for their injuries. Under this interpretation, the claim may not be in conflict with a federal law that seeks uniformity, since it would not impose an affirmative legal obligation on the defendant to take specific actions to cure its data security defects, but would simply require that the defendant compensate the plaintiffs.

⁸² The purpose of the federal law may be included in a purposes section of the text itself. .g., H.R. 1770, § 1(b) (stating the purposes of the bill). These purposes were reinforced by statements made by the Committee on Energy and Commerce as it considered the bill. See House Committee on Energy and Commerce, “Data Security and Breach Notification Act of 2015,” March 25, 2015, <https://energycommerce.house.gov/fact-sheet/data-security-and-breach-notification-act-2015> (noting that the law would create a “uniform national policy” that would “replac[e] the patchwork of state and territory laws” currently in place).

⁸³ 133 S. Ct. 2466 (2013).

⁸⁴ *Id.* at 2479-80.

⁸⁵ *Id.* at 2488 (Sotomayor, J., dissenting).

Key Takeaways on Federal Preemption of State Data Security and Breach Notification Laws

- Congress can supersede state and local laws, regulations, and common law causes of action through express preemption and/or implied preemption.
- Under express preemption, a reviewing court will closely examine the text of the express preemption clause to determine the *types* of actions that could be preempted and the *subject matter* scope of that preemption.
- All of the data security and breach notification bills include an express preemption clause.
- The text of the express preemption clause and a saving clause, if present, will determine whether state statutes, regulations, and common law causes of action regarding data security and breach notification specifically and/or consumer protection generally would be preempted.
- Even if there is an express preemption clause, state and local actions can still be superseded under implied conflict preemption.

Agency Enforcement of Data Security and Breach Notification Requirements

Another question that has arisen in the debate on federal data security and breach legislation is which federal agency should be responsible for enforcing the new requirements. The various proposals would primarily task the Federal Trade Commission (FTC) with enforcing the new requirements, but take differing approaches as to whether the Federal Communications Commission (FCC) should be permitted to retain its existing enforcement authority regarding data security and breach notification for telecommunication providers.

Current FTC Authority: Unfair or Deceptive Acts and Practices

The FTC has broad authority under Section 5 of the Federal Trade Commission Act (FTCA) to prohibit “unfair or deceptive acts or practices in or affecting commerce....”⁸⁶ Under the statute, an act or practice may be unfair if it “causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.”⁸⁷ While the FTC’s authority over unfair or deceptive practices is broad, it is not unlimited. For example, the FTC cannot use this authority to enforce against all “persons, partnerships, or corporations....” Rather, several entities are exempted from the scope of this authority,⁸⁸ including

- banks and savings and loan institutions described in 15 U.S.C. § 57a(f)(3);
- federal credit unions described in 15 U.S.C. § 57a(f)(4);
- common carriers subject to the Communications Act of 1934, as amended;⁸⁹
- common carriers subject to subtitle IV of title 49;⁹⁰

⁸⁶ 15 U.S.C. § 45(a).

⁸⁷ 15 U.S.C. § 45(n).

⁸⁸ 15 U.S.C. § 45(a)(2).

⁸⁹ 47 U.S.C. §§ 151 *et seq.* Section 5 of the FTCA exempts “common carriers subject to the Acts to regulate commerce.” 15 U.S.C. § 45(a)(2). Section 4 of the FTCA defines “Acts to regulate commerce” to include “the Communications Act of 1934 and all Acts amendatory thereof and supplementary thereto.” 15 U.S.C. § 44.

- air carriers and foreign air carriers subject to part A of subtitle VII of title 49,⁹¹ and
- persons, partnerships, or corporations subject to the Packers and Stockyards Act.⁹²

Therefore, for example, the FTC could not bring an enforcement action alleging an unfair or deceptive act or practice, engaged in as part of its common carrier activities, against a telephone company that is classified as a common carrier by the FCC under the Communications Act.

The FTC has employed its unfair or deceptive act or practice authority to bring enforcement actions and to seek settlements with companies that experience data breaches. These actions generally focus on the allegedly deceptive nature of the claims companies make about the security provided for consumers' data and/or the company's failure to reasonably safeguard consumer data that leads to a breach. For more information on the FTC's use of this authority in the data security and breach context, see CRS Report R43723, *The Federal Trade Commission's Regulation of Data Security Under Its Unfair or Deceptive Acts or Practices (UDAP) Authority*, by Gina Stevens.

Current FCC Authority

While telecommunications common carriers are not subject to the FTC's unfair or deceptive acts or practices authority, they are required to follow FCC rules relating to data security and breach notification.⁹³ Section 222 of the Communications Act establishes a duty for common carriers "to protect the confidentiality of proprietary information of... customers...."⁹⁴ Furthermore, under Section 201 of the Communications Act, common carriers must ensure that all "charges, practices, classifications, and regulations" relating to telecommunications service are just and reasonable, which the FCC has interpreted as applying to carriers' practices of protecting customers' personally identifiable information.⁹⁵

Additionally, Sections 631⁹⁶ and 338(i)⁹⁷ of the Communications Act establish more limited security rights for subscribers of cable and satellite television providers, as discussed below.

(...continued)

⁹⁰ 49 U.S.C. §§ 10101 *et seq.* Section 5 of the FTCA exempts "common carriers subject to the Acts to regulate commerce." 15 U.S.C. § 45(a)(2). Section 4 of the FTCA defines "Acts to regulate commerce" to include "subtitle IV of title 49." 15 U.S.C. § 44.

⁹¹ 49 U.S.C. §§ 40101 *et seq.*

⁹² 7 U.S.C. §§ 181 *et seq.*

⁹³ Additionally, the FTC and FCC have recently signed a Memorandum of Understanding to coordinate the agencies' activities with regard to consumer protection. FCC-FTC Consumer Protection Memorandum of Understanding, Nov. 16, 2015, http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db1116/DOC-336405A1.pdf.

⁹⁴ 47 U.S.C. § 222(a).

⁹⁵ 47 U.S.C. § 201(b); *see* In the Matter of AT&T Services, Inc., 30 FCC Rcd 2808 (April 8, 2015) *available at* <https://www.fcc.gov/document/att-pay-25m-settle-investigation-three-data-breaches> [hereinafter AT&T Consent Decree].

⁹⁶ 47 U.S.C. § 551.

⁹⁷ 47 U.S.C. § 338(i).

Common Carriers

Section 201(b) and 222 requirements apply to entities that are classified as common carriers under Title II of the Communications Act, which includes traditional telecommunications common carriers (such as telephone companies). Following the FCC's 2015 Open Internet Order,⁹⁸ in which the Commission reclassified broadband Internet access service providers (BIAS or Internet service providers) as Title II common carriers, these sections also apply to those entities, provided that the FCC's reclassification decision survives legal challenge.⁹⁹ For more information on the 2015 Open Internet Order, see CRS Report R43971, *Net Neutrality: Selected Legal Issues Raised by the FCC's 2015 Open Internet Order*, by Kathleen Ann Ruane.

Section 222 Customer Proprietary Network Information (CPNI)

Common carriers are subject to obligations derived from Section 222 of the Communications Act, which requires them to guard the confidentiality of customer proprietary network information (CPNI) and ensure that it is not disclosed to third parties without customer approval or as required by law.¹⁰⁰ CPNI is defined as

- (A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and
- (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier;

except that such term does not include subscriber list information.¹⁰¹

It includes such information as call records, location information, features of a customer's service, and billing records, among other types of data.

The FCC has issued regulations explaining common carriers' duties to protect CPNI.¹⁰² These regulations define when a carrier is permitted to use and/or share CPNI with other entities without a customer's approval and when a carrier can only use and/or share CPNI subject to a customer's

⁹⁸ In the Matter of Protecting and Promoting the Open Internet, Report and Order, FCC 15-24 (2015). The Order was subsequently published in the *Federal Register*. Protecting and Promoting the Open Internet, 80 Fed. Reg. 19737 (April 13, 2015).

⁹⁹ Numerous parties have challenged the FCC's 2015 Open Internet Order. Those cases have been consolidated in the U.S. Court of Appeals for the D.C. Circuit under the caption *United States Telecomm. Ass'n, et. al v. Federal Communications Commission*. U.S. Telecomm. Ass'n v. FCC, D.C. Cir. No. 15-1063. The Federal Register publication of the Order indicated that it would take effect on June 12, 2015. 80 Fed. Reg. 19738. Parties challenging the order filed a motion with the appellate court to stay the effective date of the order pending review. The court of appeals denied that motion, allowing the new rules to take effect on June 12. U.S. Telecomm. Ass'n v. FCC, D.C. Cir. No. 15-1063, Order Denying Motion for Stay and Granting Motion for Expedited Review (June 11, 2015), available at <http://docs.techfreedom.org/oiostaydenial.pdf>.

Assuming the Order survives legal challenges, by reclassifying BIAS as Title II common carriers, it appears as though the FTC will no longer have jurisdiction to enforce its unfair or deceptive acts or practices authority against these providers.

¹⁰⁰ 47 U.S.C. § 222.

¹⁰¹ 47 U.S.C. § 222(h)(1).

¹⁰² 47 C.F.R. §§ 64.2001 *et seq.*

opt-in or opt-out approval.¹⁰³ Carriers are also required to notify law enforcement and customers when a breach of CPNI occurs.¹⁰⁴

In its Open Internet Order, the FCC specifically declined to forbear from applying Section 222 to Internet service providers, stating:

We find that forbearance from the application of section 222 with respect to broadband Internet access service is not in the public interest... and that section 222 remains necessary for the protection of consumers... The Commission has emphasized that ‘[c]onsumers’ privacy needs are no less important when consumers communicate over and use broadband Internet access than when they rely on [telephone] services.’¹⁰⁵

While the *statutory* requirements of Section 222 apply to Internet service providers, the FCC did choose to forbear from applying its CPNI *rules* to Internet service providers.¹⁰⁶ The Commission noted that the rules would not necessarily “be well suited to broadband Internet access service” since “certain of those rules appear more focused on concerns that have been associated with voice service ... [and] do not address many of the types of sensitive information to which a provider of broadband Internet access service is likely to have access.”¹⁰⁷ However, the Commission stressed that Internet service providers must still comply with the text of the statutory provisions in Section 222.¹⁰⁸

Section 201(b) Reasonableness Requirements

The FCC has also relied on its Section 201(b) authority to bring enforcement actions against common carriers that suffer data breaches. Section 201(b) states that common carrier “charges, practices, classifications, and regulations” must be just and reasonable.¹⁰⁹ For example, in 2015, the FCC entered into a consent decree with AT&T following an investigation into the company’s alleged failure to protect the confidentiality of CPNI that led to a data breach.¹¹⁰ The FCC declared that AT&T’s “failure to reasonably secure” CPNI not only violated its duties under Section 222 but “also constitute[d] an unjust and unreasonable practice in violation of the [Communications] Act.”¹¹¹ It referenced an earlier enforcement action in which the FCC determined that a “failure to protect and secure” customers’ personally identifiable information, CPNI, and other kinds of data, was an unjust and unreasonable practice in violation of Section 201(b).¹¹² This failure was evidenced in part by the fact that the carrier did not encrypt any of its customers’ data that was stored on servers accessible over the public Internet.¹¹³ Along with Section 222, Section 201(b)’s reasonableness requirement appears to be another tool the FCC can use to hold carriers accountable for certain data security and breach failures.

¹⁰³ 47 C.F.R. §§ 64.2005, 64.2007.

¹⁰⁴ 47 C.F.R. § 64.2011.

¹⁰⁵ 80 Fed. Reg. 19814.

¹⁰⁶ 80 Fed. Reg. 19815.

¹⁰⁷ *Id.*

¹⁰⁸ 80 Fed. Reg. 19814-19815.

¹⁰⁹ 47 U.S.C. § 201(b).

¹¹⁰ AT&T Consent Decree, *supra* note 95, at 2808.

¹¹¹ *Id.*

¹¹² In the Matter of TerraCom, Inc. and YourTel America, Inc. Apparent Liability for Forfeiture, 29 FCC Rcd 13325, 13335-36 (2014).

¹¹³ *Id.* at 13336.

Cable and Satellite Providers

Several statutory provisions also impose data security requirements on cable and satellite television providers. Section 631 of the Communications Act prohibits a cable operator from using a cable system “to collect personally identifiable information concerning a subscriber without the prior written or electronic consent of the subscriber concerned.”¹¹⁴ Furthermore, cable operators are forbidden from disclosing a subscriber’s personally identifiable information without the subscriber’s consent (with limited exceptions) and must “take such actions as are necessary to prevent unauthorized access to such information” by a third party.¹¹⁵ Similar provisions apply to satellite television carriers.¹¹⁶ These data security requirements for cable and satellite operators include protections for a subscriber’s viewing history.¹¹⁷

Key Takeaways on Agency Enforcement Roles

- Both the FTC and the FCC have interpreted their statutory authority to permit enforcement actions against entities that have poor data security practices and experience data breaches.
- The FTC brings enforcement actions under its “unfair or deceptive acts or practices” authority in the FTC Act. However, this authority does not allow the FTC to bring enforcement actions against common carriers (as classified by the FCC under the Communications Act) that experience data breaches while engaging in common carrier activities.
- The FCC brings enforcement actions against common carriers under its rules for protecting customer proprietary network information (CPNI) and a provision of the Communications Act that requires “charges, practices, classifications, and regulations” to be just and reasonable.
- The FCC also has rules governing the disclosure of customer information that apply to cable and satellite providers.
- Several data security and breach notification bills would alter these existing authorities—either expanding the FTC’s authority to include common carriers and eliminating the FCC’s authority or expanding the FTC’s authority while leaving the FCC’s rules untouched.

Proposed Changes to FTC and FCC Enforcement Authority

Several of the bills being considered in the 114th Congress propose changes to the FTC and FCC’s existing enforcement authority regarding data security and/or breach notification, while two others would leave the current system essentially unaltered.¹¹⁸ Under the bills that propose no changes to enforcement authority, common carriers under the Communications Act would not be

¹¹⁴ 47 U.S.C. § 551(b).

¹¹⁵ 47 U.S.C. § 551(c). The FCC recently entered into a consent decree with Cox Communications, Inc., representing its first enforcement action against a cable operator regarding a data breach. In the Matter of Cox Communications, Inc., 2015 FCC LEXIS 3412 (Nov. 5, 2015), available at https://apps.fcc.gov/edocs_public/attachmatch/DA-15-1241A1.pdf.

¹¹⁶ 47 U.S.C. § 338(i).

¹¹⁷ 47 U.S.C. §§ 338(i)(4)(B)(iii), 551(c)(2)(C). A person aggrieved by a violation of section 631 or 338(i) may bring a civil action in a federal district court seeking actual damages, punitive damages, and attorneys’ fees. 47 U.S.C. §§ 338(i)(7), 551(f).

¹¹⁸ H.R. 580 and S. 177 make requirements for data security and breach notification applicable only to those entities already subject to FTC unfair and deceptive acts or practices enforcement, with limited exceptions. H.R. 580, § 4(a)-(b); S. 177, § 5(a), (c). S. 177 applies its new requirements to non-profit entities, notwithstanding the existing limits on FTC enforcement authority in 15 U.S.C. §§ 44, 45(a)(2). S. 177, § 5(a)(2). It also includes an “opt-in” provision that would allow entities that are not automatically covered to voluntarily enter into an agreement with the FTC to be bound by the bill’s breach notification requirements. *Id.* at § 5(b).

subject to new data security and breach notification requirements, since they are not subject to FTC unfair or deceptive acts or practices authority. Common carriers would continue to be subject to Sections 201(b) and 222, as enforced by the FCC. Alternatively, cable and satellite providers would be subject to both the bills' new requirements, because they fall within the FTC's unfair or deceptive acts or practices authority, and Section 338(i) or 631, as applicable.

Some of the bills that propose changes to the current agency enforcement structure would expand the FTC's jurisdiction and leave the FCC's existing statutory and regulatory authority intact.¹¹⁹ For example, under H.R. 1704, the FTC would enforce the new requirements "in the same manner, by the same means, and with the same jurisdiction, powers, and duties" as it has under the FTCA, except that the exceptions to its Section 5 authority "shall not apply."¹²⁰ The bill does not alter the FCC's authority under Sections 201, 222, 338(i), or 631, although it does require the FTC to consult with the FCC before promulgating rules regarding an entity within the FCC's jurisdiction.¹²¹ If this type of bill were enacted, common carriers and cable and satellite providers would all be subject to both the new requirements in the bill, as enforced by the FTC, and the FCC's existing requirements.

Alternatively, some bills both expand the FTC's jurisdiction and eliminate some or all of the FCC's authority to regulate in this area.¹²² For example, H.R. 1770 states that,

as sections 201, 202, 222, 338, and 631 of the Communications Act of 1934... and any regulations promulgated thereunder, apply to covered entities with respect to securing information in electronic form from unauthorized access, including notification of unauthorized access to data in electronic form containing personal information, such sections and regulations promulgated thereunder *shall have no force or effect*, unless such regulations pertain solely to 9–1–1 calls.¹²³

Under this bill, with the exception of regulations pertaining solely to 911 calls, the FCC retains no authority to enforce its requirements under Sections 201, 222, 338, and 631.¹²⁴ Therefore, if this type of bill were enacted, common carriers and cable and satellite providers would be subject to the new requirements, as enforced by the FTC, but would no longer have to comply with the FCC requirements. Other bills only eliminate the FCC's ability to enforce *some* of the relevant Communications Act provisions regarding data security and breach notification, but not all.¹²⁵

¹¹⁹ *E.g.*, H.R. 1704, § 107; S. 1158, §§ 203(d), 218(d). H.R. 1704 also requires the FTC to consult with the FCC if its enforcement action involves a business entity subject to the FCC's authority. H.R. 1704, § 107(c). S. 1158 specifically preserves the FCC's authority by stating that "[n]othing in this Act may be construed in any way to limit the authority of the Federal Communications Commission under any other provision of law." S. 1158, § 220(e).

¹²⁰ H.R. 1704, § 107(b).

¹²¹ *Id.* at § 107(f)(2).

¹²² H.R. 1053, § 171(c); H.R. 1770, § 6(c); H.R. 2205, § 5(b); S. 547, § 171(c); S. 961, § 5(b); S. 1027, § 4(b).

¹²³ H.R. 1770, § 6(c)(1) (emphasis added).

¹²⁴ *Id.*

¹²⁵ H.R. 1053 and S. 547 state that "If a person is subject to a provision of section 222 or 631 of the Communications Act of 1934... and a provision of this title, such provision of such section 222 or 631 shall not apply to such person to the extent that such provision of this title applies to such person." H.R. 1053, § 171(c); S. 547, § 171(c). These bills do not appear to alter the validity of Sections 201 or 338 of the Communications Act. S. 1027 states that "Sections 222, 338, and 631 of the Communications Act of 1934... and any regulations promulgated thereunder, shall not apply with respect to the information security practices, including practices relating to the notification of unauthorized access to data in electronic form, of any covered entity otherwise subject to those sections." S. 1027, § 4(b). This bill does not appear to alter the validity of Section 201 of the Communications Act.

Removing the FCC's authority in this area may reduce the types of data that are subject to security and breach notification requirements, as compared with a proposal that imposes new requirements while maintaining the FCC's authority. For example, data within the existing definition of CPNI may not meet the definition of "covered information" in the federal proposal, and, therefore, may not be subject to the new federal standards nor the security and breach notification requirements in the CPNI rules, if those rules have "no force or effect" going forward.

Proponents of bills that reduce or eliminate the FCC's authority in this subject area have emphasized the benefits of imposing a uniform, predictable standard across all covered entities.¹²⁶ Opponents of this approach argue that restricting FCC authority weakens consumer protection by eliminating clear, predictable rules with which companies are accustomed to complying.¹²⁷ Some also argue that the type of data to be protected under new federal requirements would be more limited than the data protected under the Communications Act provisions and, therefore, eliminating the FCC's ability to enforce those provisions will reduce consumers' data protection.¹²⁸ These issues are likely to continue to be discussed as the bills are considered in the 114th Congress.

Author Contact Information

Alissa M. Dolan
Legislative Attorney
adolan@crs.loc.gov, 7-8433

¹²⁶ See House Energy and Commerce Committee, "Data Security and Breach Notification Act of 2015," March 25, 2015, available at <http://energycommerce.house.gov/fact-sheet/data-security-and-breach-notification-act-2015> (noting that the draft bill that eventually became H.R. 1770 is "designed to create a uniform national policy ...").

¹²⁷ Testimony of Laura Moy, Senior Policy Counsel, New America's Open Technology Institute, Before the House Energy and Commerce Committee, Subcommittee on Commerce, Manufacturing, and Trade, "Discussion Draft of H.R. ___, Data Security and Breach Notification Act of 2015," March 18, 2015, available at <http://docs.house.gov/meetings/IF/IF17/20150318/103175/HHRG-114-IF17-Wstate-MoyL-20150318.pdf> ("The FCC's robust rules promulgated under that authority require telecommunications carriers to, among other things, train personnel on customer proprietary network information (CPNI), have an express disciplinary process in place for abuses, and annually certify that they are in compliance with the CPNI rules... [T]he specific data security requirements imposed by the FCC[] would all be eliminated by this bill and replaced with the less specific 'reasonableness' standard... The consumer protections provided by the Communications Act are of critical importance to consumers, and appropriately overseen by an agency with decades of experience regulating entities that serve as gatekeepers to essential communications networks. This bill threatens to eliminate core components of those protections...." (internal citations omitted)).

¹²⁸ Letter to Chairman Fred Upton and Ranking Member Frank Pallone from numerous consumer groups, Re: the Data Security and Breach Notification Act (H.R. 1770), available at http://www.consumerfed.org/pdfs/150409_Data-Security-Breach_letter.pdf. The letter argues that

The Communications Act contains very strong data security and breach notification protections for information about customers' use of telecommunications services. It also protects cable and satellite subscribers' information, including their viewing histories. But as with email login information and health records, this bill is too narrow to cover all telecommunications usage information, and it would not protect cable and satellite viewing histories at all. The bill would simply eliminate data security and breach notification protections for sensitive information about use of these services. In addition, the breach notification and data security protections in this bill are weaker than existing law under the Communications Act.

Id. at 2.



Ingestibles, Wearables and Embeddables

Routine tests can be anything but. Appointment times are often inconvenient. You may be at the mercy of walk-in labs and testing facilities, where waiting could be uncertain and often longer than many people can accommodate. Personal health – which should be a top priority – can suffer when important diagnostic tests fall off our to-do lists.

Recent advances in broadband-enabled sensor technology offer the potential for the emergence of more convenient, ultimately less-costly – and less-invasive – solutions. For example, we may soon see widespread use of smart clothing (or smart “tattoo” applications) that use skin-based sensors to measure things like heart rate, respiration and blood pressure. These new types of technologies are generically called “ingestibles,” “wearables” and “embeddables.”



Ingestibles are broadband-enabled digital tools that we actually “eat.” For example, there are “smart” pills that use wireless technology to help monitor internal reactions to medications. Or imagine a smart pill that tracks blood levels of medications in a patient’s body throughout the day to help physicians find optimum dosage levels, avoid overmedicating, and truly individualize treatment. Also, miniature pill-shaped video cameras may one day soon replace colonoscopies or endoscopies. Patients would simply swallow a “pill,” which would collect and transmit images as it makes its way through the digestive system.



Wearables are digital tools you can “wear,” such as wristwatch-like devices that have sensors to monitor your heart rate and other vital signs. Beyond medical monitoring, such wearables may also help improve athletic performance, track fitness goals or help prevent dangerous falls in the elderly. In fact, designers are now able to put sensors in T-shirts and other clothing to monitor perspiration as a stress indicator. And, “tattoo-like” sensors that could be peeled off after use or that might be absorbed by the body are another similar advance. These sensors gather data through skin contact and transmit information wirelessly to smartphones and remote diagnostic facilities.



Embeddables are miniature devices that are actually inserted under the skin or deeper into the body. A heart pacemaker is one kind of embeddable device. In the future, embeddables may use nanotechnology and be so tiny that doctors would simply “inject” them into our bodies. Some promising applications in this area could help diabetes patients monitor their blood sugar levels reliably and automatically, without the need to prick their fingers or otherwise draw blood.



Want to Know More? The Connect2Health^{fcc} Task Force is working to raise consumer awareness about the value of broadband in the health and care sectors. Learn about the FCC’s Connect2Health Task Force and its work on consumer health issues at www.fcc.gov/health. For information about other communications issues, visit the FCC’s Consumer website at www.fcc.gov/consumers.

For this or any other consumer publication in an accessible format (electronic ASCII text, Braille, large print or audio), please write or call us at the address or phone number below, or send an email to FCC504@fcc.gov. This document is for consumer education purposes only and is not intended to affect any proceedings or cases involving this subject matter or related issues.



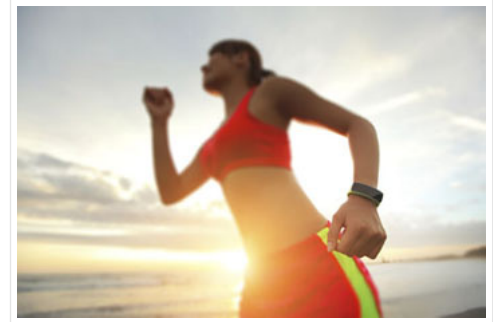
Wearable Computers and Wearable Technology

What are wearable computers and wearable technology?

Wearable computers and wearable technology are small devices using computers and other advanced technology that are designed to be worn in clothing or directly against the body. These devices are usually used for entertainment and other tasks like monitoring physical activity.

Wearable technology typically uses low-powered radiofrequency (RF) transmitters to send and receive data from smartphones or the Internet. RF transmitters emit radiowaves, a type of non-ionizing radiation.

Most devices use low-powered Bluetooth technology similar to that used in “hands free” headsets for cell phones and many other wireless consumer devices. Some devices may use Wi-Fi or other communication technologies as well.



What are some examples of wearable computers and wearable technology?

Familiar examples of wearable computers or wearable technology include “smartwatches” and fitness trackers. Future devices could include head-mounted displays and a wide variety of personal health monitors.

Wearable Technology and Safety

RF transmitters in wearable technology expose the user to some level of RF radiation. RF radiation is a form of non-ionizing radiation made up of radiowaves.

[For more information on non-ionizing radiation, click here](#)

RF transmitters in wearable devices operate at extremely low power levels and normally send signals in streams or brief bursts (pulses) for a short period of time. As a result, wearable devices expose the user to very small levels of RF radiation over time.

[For more information on non-ionizing radiation and possible health effects, click here](#)

How much RF radiation am I exposed to?

To be sold in the U.S., equipment that transmits RF radiation must meet exposure limits set by the Federal Communications Commission (FCC). These limits are designed to reduce exposure to RF radiation.

[For more information on FCC regulations around RF radiation, click here \(https://www.fcc.gov/encyclopedia/radio-frequency-safety\)](https://www.fcc.gov/encyclopedia/radio-frequency-safety)

While the FCC guidelines were adopted in 1996, they are similar to international guidelines that are presently in effect in many other countries. Wearable devices expose the user to small amounts of RF radiation compared to these international exposure limits (<http://www.icnirp.org/cms/upload/publications/ICNIRPemfgdl.pdf>).

Wearable technology can distract you

If you use wearable devices, it could be a source of distraction and raise a number of safety and other issues unrelated to RF radiation exposure. This is a major concern if you are driving a car or participating in other activities that require close attention.

What You Need to Know

- Most wearable devices include low-powered RF transmitters to enable them to communicate with other devices.
- To be sold in the U.S., all such devices must meet FCC limits for human exposure to RF radiation.
- Wearable devices expose the user to lower amounts of RF radiation compared to international exposure limits.
- Wearable electronics may distract the user and increase the chances of injury while driving or using dangerous equipment.
- CDC continues to monitor this topic.

More Information

[The Federal Communications Commission \(FCC\) \(http://www.fcc.gov/\)](http://www.fcc.gov/)

[CDC – Workplace Safety and Health Topics: EMF \(Electric and Magnetic Fields\) \(http://www.cdc.gov/niosh/topics/emf/\)](http://www.cdc.gov/niosh/topics/emf/)

[CDC- Frequently Asked Questions about Cell Phones and Your Health](#)

[NIH – Cell Phones \(http://www.niehs.nih.gov/health/topics/agents/cellphones/index.cfm\)](http://www.niehs.nih.gov/health/topics/agents/cellphones/index.cfm)

Warning Letters Highlight Differences Between Cosmetics and Medical Devices

FDA warning letters issued to manufacturers and/or distributors of devices marketed for regrowing hair, weight reduction, spider vein removal, and dermabrasion, as well as injectable fillers and decorative contact lenses illustrate an important legal distinction – the differences between the legal definitions of cosmetics and medical devices.

Although the devices cited in these warning letters are intended to affect a person's appearance, the fact that they are intended to diagnose or treat a medical condition or affect the structure or function of the body makes them medical devices under the **Federal Food, Drug, & Cosmetic Act** (<http://wcms.fda.gov/FDAgov/RegulatoryInformation/Legislation/FederalFoodDrugandCosmeticActFDCA/default.htm>) (FD&C Act).

The FD&C Act requires medical device manufacturers to obtain marketing clearance for their products before offering them for sale [FD&C Act, section 501(f)(1)]. The law does not require clearance or approval to market cosmetic products or ingredients. (An exception is **color additives** ([/ForIndustry/ColorAdditives/default.htm](http://wcms.fda.gov/FDAgov/RegulatoryInformation/Legislation/FederalFoodDrugandCosmeticActFDCA/default.htm)), which are covered separately in section 721 of the FD&C Act.) In addition, medical devices are subject to the Quality System Regulation (21 CFR part 820). Cosmetics are not subject to this regulation.

This is how the FD&C Act defines a medical device:

"...an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including any component, part, or accessory, which is - (1) recognized in the official National Formulary, or the United States Pharmacopeia, or any supplement to them, (2) intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals, or (3) intended to affect the structure or any function of the body of man or other animals, and which does not achieve its primary intended purposes through chemical action within or on the body of man or other animals and which is not dependent upon being metabolized for the achievement of its primary intended purposes." [FD&C Act, section 201 (h)]

In addition, under the FD&C Act, all contact lenses are medical devices, [FD&C Act, section 520(n)], not cosmetics.

This is how the FD&C Act defines a cosmetic:

"...(1) articles intended to be rubbed, poured, sprinkled, or sprayed on, introduced into, or otherwise applied to the human body or any part thereof for cleansing, beautifying, promoting attractiveness, or altering the appearance, and (2) articles intended for use as a component of any such articles; except that such term shall not include soap." [FD&C Act, section 201(i)]

FDA regulates false eyelashes and artificial nails, for example, as cosmetics. The **Consumer Product Safety Commission** (<http://www.cpsc.gov/>) has jurisdiction over many non-medical devices that people use to affect their appearance, such as manicure tools, hair dryers, cotton-tipped swabs, razors and electric shavers. For related information, see **Is It a Cosmetic, a Drug, or Both? (or Is It Soap?)** ([/Cosmetics/GuidanceRegulation/LawsRegulations/ucm074201.htm](http://www.fda.gov/oc/ohrt/cosmetics/guidance/regulation/laws/regulations/ucm074201.htm)), **Cosmeceuticals** ([/Cosmetics/Label-](http://www.fda.gov/oc/ohrt/cosmetics/guidance/regulation/laws/regulations/ucm074201.htm)

[ing/Claims/ucm127064.htm](#)), [Soap \(/Cosmetics/ProductsIngredients/Products/ucm115449.htm\)](#), [Warning Letters \(/ICECI/EnforcementActions/WarningLetters/default.htm\)](#), and [Medical Devices \(/MedicalDevices/default.htm\)](#).

- [Eclipse Aesthetics LLC \(/ICECI/EnforcementActions/WarningLetters/2016/ucm500631.htm\)](#) March 28, 2016
- [Eclipse Aesthetics LLC \(/ICECI/EnforcementActions/WarningLetters/2015/ucm480331.htm\)](#) October 27, 2015
- [Medica Outlet \(http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2015/ucm449803.htm\)](#) June 1, 2015
- [Dr. Ashley Minas \(http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2015/ucm449703.htm\)](#) May 29, 2015
- [Dr. Hettie Morgan \(http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2015/ucm449730.htm\)](#) May 29, 2015
- [Jian Peng Zhou \(http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2015/ucm449545.htm\)](#) May 29, 2015
- [9mm Special Effects \(http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/2015/ucm448437.htm\)](#) May 19, 2015
- [Derma Pen, LLC \(/ICECI/EnforcementActions/WarningLetters/2015/ucm429899.htm\)](#) January 9, 2015
- [Lucky Beauty Equipment Co., Ltd. \(http://www.fda.gov/ICECI/EnforcementActions/WarningLetters/ucm382779.htm\)](#) January 15, 2014
- [BNB Medical Co., Ltd. \(ssLINK/ucm252103.htm\)](#) April 19, 2011
- [Refine USA, LLC \(ssLINK/ucm252088.htm\)](#) April 18, 2011
- [Gaunitz Hair Sciences, LLC \(ssLINK/ucm1048189.htm\)](#) August 7, 2008
- [Sunetics International Corporation \(ssLINK/ucm1048188.htm\)](#) August 7, 2008

More in [Warning Letters \(/Cosmetics/ComplianceEnforcement/WarningLetters/default.htm\)](#)



FOSTERING THE ADVANCEMENT OF THE INTERNET OF THINGS

THE DEPARTMENT OF COMMERCE
INTERNET POLICY TASK FORCE &
DIGITAL ECONOMY LEADERSHIP TEAM

January 2017

TABLE OF CONTENTS

TABLE OF CONTENTS	i
1. Executive Summary.....	1
2. The Internet of Things (IoT) Landscape	3
A. Unique Opportunities and Challenges	3
B. Describing IoT	5
C. Benefits of IoT	8
D. Role of Government in Fostering IoT.....	10
i. International Engagement.....	12
ii. Stakeholder-Driven Policy Processes	13
3. An Approach for Departmental Action to Advance the Internet of Things	14
4. Areas of Engagement.....	16
A. Enabling Infrastructure Availability and Access	16
i. Increased Infrastructure Demand.....	16
ii. Increased Spectrum Demand	17
iii. Internet Protocol Version 6 Adoption	19
iv. Issues of Equity in IoT.....	20
v. Planned Activities.....	20
1. Current Initiatives	21
2. Proposed Next Steps	23
B. Crafting Balanced Policy and Building Coalitions.....	24
i. Cybersecurity.....	24
1. Need for Flexible, Risk-based Solutions	25
2. Security by Design.....	27
3. Patching.....	28
4. Technical Limitations	29
ii. Privacy	30
iii. Intellectual Property	33
1. Copyright	34
2. Patents.....	36

3.	Trade Secrets.....	38
4.	Trademark.....	39
iv.	Free Flow of Data Across Borders.....	39
v.	Planned Activities.....	40
1.	Current Initiatives.....	40
2.	Proposed Next Steps.....	42
C.	Promoting Standards and Technology Advancement.....	44
i.	Standards Development.....	44
ii.	Planned Activities.....	47
1.	Current Initiatives.....	47
2.	Proposed Next Steps.....	48
D.	Encouraging Markets.....	49
i.	Public-Private Partnerships and Government Procurement.....	49
ii.	Workforce Issues: Education, Training, and Civil Liberties.....	49
iii.	Quantifying the IoT Sector.....	51
iv.	Planned Activities.....	51
1.	Current Initiatives.....	52
2.	Proposed Next Steps.....	53
5.	Conclusion.....	54
	Appendix A: Proposed Next Steps.....	56
	Appendix B: Questions for Further Discussion.....	60
	Appendix C: Acknowledgements, Workshop Panelists, and Request for Comment Respondents.....	61

1. Executive Summary

The Internet of Things (IoT) – in which connected devices are proliferating at an unprecedented rate – is a technological development that is transforming the way we live and do business. IoT continues the decades-long trend of increasing connectivity among devices and the Internet, bringing online everything from refrigerators to automobiles to factory inventory systems. At the same time, IoT encompasses a widening scope of industries and activities and a vastly increasing scale and number of devices being connected, thus raising the stakes and impacts of broad connectivity.

The prospective benefits of IoT to personal convenience, public safety, efficiency, and the environment are clear. IoT has the potential to make our highways safer by enabling connected vehicles to interact with each other to prevent accidents, to make quality health care more accessible through remote monitoring devices and telehealth practices for those who cannot easily travel, and to reduce waste and improve efficiency both in factory supply chains and in the running of cities. It even has the potential to create new industries and consumer goods that have yet to be imagined. For the full potential to be realized, however, the necessary infrastructure and policies must be in place, including strategies to respond to the challenges raised in areas such as cybersecurity and privacy.

Due to its expertise in the issues raised by IoT, as well as its economy-wide perspective, the Department of Commerce (Department) is well placed to meet these challenges and to champion the development of a robust IoT environment that benefits consumers, the economy, and society as a whole.

With an April 2016 Request for Comment, “The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things,”¹ the Department of Commerce sought to review the current technological and policy landscape relating to IoT. A broad array of stakeholders – from the private sector, academia, government, and civil society – offered perspectives² in response to the request. In September 2016, the Department hosted a workshop³ to delve deeper into the questions raised by the Request for Comment, and to explore some of the related issues arising from the public comments.

This paper represents the Department’s analysis of those comments. It also identifies key issues that can impact the deployment of IoT technologies, highlights potential benefits and challenges, and discusses what role, if any, the U.S. Government, particularly the Department of Commerce, should play in this evolving landscape.

¹ See <https://www.federalregister.gov/d/2016-07892>

² See <https://ntia.doc.gov/federal-register-notice/2016/comments-potential-roles-government-fostering-advancement-internet-of-things>

³ See <https://ntia.doc.gov/other-publication/2016/09012016-fostering-advancement-internet-things-workshop-webcast>

Over the past few decades in the United States, the role of government largely has been to establish and support an environment that allows technology to grow and thrive. Encouraging private sector leadership in technology and standards development, and using a multistakeholder approach to policy making, have been integral elements of the government’s approach to technology development and growth. Following a review of public comments, meetings with stakeholders, and the public workshop, it is clear that while specific policies may need to be developed for certain vertical segments of IoT, the challenges and opportunities presented by IoT require a reaffirmation rather than a reevaluation of this well-established U.S. Government policy approach to emerging technologies.

The goal of this paper is to identify elements of an approach for the Department of Commerce to foster the advancement of the Internet of Things. The record of comments underlying this green paper, however, does set forth a series of issues that should be considered in any future discussions related to the possibility of a national IoT strategy. The Department heard a strong message from the submitted comments that coordination among U.S. Government partners would be helpful, because of the complex, interdisciplinary, cross-sector nature of IoT. A federal coordination structure for these issues may also be helpful when working with international and private sector partners.

This paper begins with an overview of IoT, including definitional issues, the benefits of IoT, the possible role of government in fostering the IoT environment, and some of the international considerations that, due to the global nature of the Internet and connected technologies, are inherent in the issues discussed in the rest of the paper. The next section lays out an approach for Departmental action organized around four engagement areas. The section thereafter provides a review and analysis of the comments, current Department initiatives, and next steps for each engagement area. Consistent with the established U.S. Government policy approach to emerging technology, this approach proposes the following principles:

-
- ❖ The Department will lead efforts to ensure the IoT environment is **inclusive and widely accessible** to consumers, workers, and businesses;
 - ❖ The Department will recommend policy and take action to support a **stable, secure, and trustworthy** IoT environment;
 - ❖ The Department will advocate for and defend a **globally connected, open, and interoperable** IoT environment built upon industry-driven, consensus-based standards; and
 - ❖ The Department will encourage IoT **growth and innovation** by encouraging expanding markets and reducing barriers to entry, and by convening stakeholders to address public policy challenges.
-

The approach identifies four broad areas of engagement to advance these principles:

- **Enabling Infrastructure Availability and Access:** Fostering the physical and spectrum-related assets needed to support IoT growth and advancement.
- **Crafting Balanced Policy and Building Coalitions:** Removing barriers and encouraging coordination and collaboration; influencing, analyzing, devising, and promoting norms and practices that will protect IoT users while encouraging growth, advancement, and applicability of IoT technologies.
- **Promoting Standards and Technology Advancement:** Ensuring that the necessary technical standards are developed and in place to support global IoT interoperability and that the technical applications and devices to support IoT continue to advance.
- **Encouraging Markets:** Promoting the advancement of IoT through Department usage, application, iterative enhancement, and novel usage of the technologies; and translating the economic benefits and opportunities of IoT to foreign partners.

The approach proposes engagement on a set of cross-cutting issues across these contexts from cybersecurity and privacy to innovation and intellectual property, with all stakeholders at the local, tribal, state, federal, and international levels. The green paper delves in depth into each of these areas of engagement, summarizing commenter feedback, describing current DOC initiatives, and proposing next steps (summarized in Appendix A: Proposed Next Steps).

The publication of this green paper will be followed by a further Request for Comment that will solicit feedback on the findings of the paper and the proposed approach and next steps. This further consultation will inform the Department's approach and next steps as we work with interagency partners on the U.S. Government's approach to IoT.

2. The Internet of Things (IoT) Landscape

A. Unique Opportunities and Challenges

The Request for Comment's initial question – and likely the most important one – was whether IoT is different from technological issues that we as a society have already faced, or at least different enough to merit specific attention and/or different policy responses. Based on the collective comments, the responses at the workshop, and our conversations with stakeholders we have concluded that IoT *is* different in important aspects:

- 1) **Scope:** IoT is connecting a wider range of systems and devices than ever before, enabling greater integration of previously distinct industries, sectors, and activities. This will require new forms of cross-sector and cross-government collaboration, knowledge sharing, and alignment. From wearable devices that track infant heartbeats to supply chains that are capable of tracking an individual soda can from production to recycling, from connected vehicles to self-monitoring bridges, IoT portends significant and in some

cases revolutionary changes. IoT applications offer the potential for industry, government, and individuals to reap benefits in terms of increased efficiency, safety, and convenience that were previously impossible. At the same time, these industries and government agencies – and society as a whole – will need to grapple with issues that are inherent to connectivity: cybersecurity, access, data flows, education, workforce and labor impacts, cultural and socio-political differences, intellectual property rights, and privacy.

- 2) **Scale:** The number of connected devices coming online is growing rapidly. Cisco estimates that, between the years of 2015 and 2020, the number of connected devices in the United States will nearly double from 2.3 billion to 4.1 billion; globally connected devices will increase from 16 billion to 26 billion over the same period.⁴ McKinsey Global Institute has projected that, by 2025, the overall impact of these devices on the global economy will be between \$4 trillion and \$11 trillion.⁵ This rapidly changing environment will have broad implications. As described by commenters, the sheer magnitude of IoT devices connected will impose significant challenges for the current infrastructure, including stability, capacity, resilience, policy and regulatory consistency, and international cooperation.
- 3) **Stakes:** While many commenters argued that IoT is an evolution rather than a revolution in information and communications technologies,⁶ the increased scale and scope produces a qualitative change in the stakes involved in connectivity. A major Internet outage or a cyberattack would never have been without consequence, but IoT raises the stakes significantly, as such events can now affect medical devices, supply chain reliability, and cars driving down the highway, raising the real possibility of physical harm.⁷ This represents a shift in the potential physical effects of incidents which, in the past, were generally isolated to industrial control system environments. Similarly, it is more important than at any time in the past to ensure that current and future policies foster an innovative and adaptive environment to realize the full potential of technology. As one commenter noted, the importance of well-crafted policy to address potential

⁴ Cisco, VNI Complete Forecast Highlights Tool (2016), http://www.cisco.com/c/m/en_us/solutions/service-provider/vni-forecast-highlights.html (“Global” and “United States” selected).

⁵ McKinsey Global Institute, Unlocking the Potential of the Internet of Things (June 2015), <http://www.mckinsey.com/business-functions/business-technology/our-insights/the-Internet-of-things-the-value-of-digitizing-the-physical-world>.

⁶ See, e.g. Ligado Networks Comment at 8; 5G Americas Comment at 3; Cisco Systems Comment at 2. See also, comments of John Godfrey, Samsung, Fostering the Advancement of the Internet of Things Workshop, September 1, 2016, Transcript, 81, <https://www.ntia.doc.gov/files/ntia/publications/09012016-iot-workshop.pdf>. For a thorough discussion of this argument, see Steve Case, *The Third Wave*, Simon and Schuster (April 2016).

⁷ *The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things NOI*, 81 Fed. Reg. at 19956-02. For views of respondents on this point, see Future of Privacy Forum Comment at 5.

barriers to adoption, innovation, and trust will only increase as more devices gain connectivity.⁸

The Department believes that IoT poses qualitatively different opportunities and challenges from those that society has dealt with before. This is because the existing opportunities and challenges of the Internet are emerging in new contexts, with greater reach and impact. These characteristics of IoT support a strong case for the U.S. Government both to pursue policies that foster IoT innovation and growth, and to promote consumer trust and safety. At the same time, it is also important to recognize the policies and practices the U.S. Government has followed for decades to create environments in which emerging technologies have thrived, and to acknowledge that those policies and practices form a strong and essential foundation for developing approaches that advance IoT applications.

B. Describing IoT

There was no consensus among commenters on a formal definition of IoT, or even on whether a common definition would be useful.⁹ Definitions vary across industry and across parts of government; the Department agrees with the commenters that emphasized the need to allow the IoT environment to grow without the restrictions of labels or specific definitions that could inadvertently limit the applications, innovations, and overall potential of IoT.¹⁰ Microsoft asserts that:

IoT is surrounded by definitional challenges. There is no universally agreed-on definition of IoT, just as there is not universal agreement that the phenomenon itself is named IoT. Rather than defining IoT narrowly, in a manner that may limit the scope of its potential applications, we urge NTIA to consider recognizing that the term IoT does not simply describe a new type of technical architecture, but a new concept that defines how we interact with the physical world.¹¹

⁸ Samsung Comment (June 2, 2016) at 1.

⁹ There is lack of consensus among stakeholders between the terms “cyber-physical systems” (CPS) and IoT. In a NIST-coordinated effort, stakeholders have chosen to define cyber-physical systems as “smart systems that include engineered interacting networks of physical and computational components,” and noted that “[t]here is significant overlap between these concepts, in particular CPS and IoT, such that CPS and IoT are sometimes used interchangeably; therefore, the approach described in this CPS Framework should be considered to be equally applicable to IoT” (<https://pages.nist.gov/cpspwg/>). A NIST publication also describes a concept labeled “Network of Things,” which can include IoT and is composed of sensors, aggregators, communication channels, an eUtility, and a decision trigger (NIST 800-183; <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf>).

¹⁰ See, e.g., State of Illinois Comment at 8-9; Trans-Atlantic Business Council Comment at 2; United States Council for International Businesses Comment at 2, 7; Verizon Comment at 4-5; Association for Computing Machinery U.S. Public Policy Council Comment at 3.

¹¹ Microsoft Comment at 3.

The U.S. Council for International Business suggested that “a precise, exclusive definition of the IoT is not necessary at this point,”¹² and the Trans-Atlantic Business Council advocated that “[a]ny definition should be flexible enough to adapt as IoT further develops.”¹³

Many commenters suggested a definition based on particular attributes of devices, activities, or the integration of sensors, actuators, and/or network connectivity.¹⁴ IBM referred to IoT “as the growing range of Internet-connected devices that capture or generate an enormous amount of data every day along with the applications and services used to interpret, analyze, predict and take actions based on the information received.”¹⁵ The Center for Data Innovation commented that IoT is device-based, with the “term used to describe the set of physical objects embedded with sensors or actuators and connected to a network.”¹⁶ Vodafone commented that it does not focus on the devices, but rather describes IoT as a “dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols” that connects to smart ‘things.’¹⁷

Other commenters did not focus on connectivity in their proposed definitions. The American Bar Association Section of Science & Technology Law argued that “IoT is not itself a ‘thing,’ device or product,” but rather “it is a conceptual structure consisting of tangible things (e.g., commercial and consumer goods containing sensors), real estate and fixtures (e.g., roads and buildings containing sensors), plus intangibles (e.g., software and data), plus a range of services (e.g., transmission, development, access contracts, etc.).”¹⁸ The Center for the Development and Application of Internet of Things Technologies at Georgia Tech stated that “of all the many facets of the Internet of Things as it is understood today, the one single groundbreaking element is not the connectivity ... [but] the smartness of things.”¹⁹ The President’s National Security Telecommunications Advisory Committee, in its 2014 Report to the President on the Internet of Things, described IoT as “a decentralized network of objects, applications, and services that can sense, log, interpret, communicate, process, and act on a variety of information or control devices in the physical world.”²⁰ Others have suggested that IoT should be described through the lens of its integrated component layers – applications, network, devices, and data – as a way to segment and analyze the associated opportunities and policy challenges.

¹² U.S. Council for International Business Comment at 2.

¹³ Trans-Atlantic Business Council Comment at 2.

¹⁴ *See, e.g.*, Dr. Cees J.M. Lanting Comment at 4; Dr. Robert Marcus Comment at 26.

¹⁵ IBM Comment at 9.

¹⁶ Center for Data Innovation Comment at 8.

¹⁷ Vodafone US Comment at 88.

¹⁸ American Bar Association Section of Science & Technology Law Comment at 15.

¹⁹ Alain Louchez Comment at 2.

²⁰ NSTAC Report to the President on the Internet of Things (2014),

<http://www.dhs.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20the%20Internet%20of%20Things%20Nov%202014%20%28updat%20%20%20.pdf>.

The growing number of sectors deploying IoT devices includes agriculture, defense, energy, entertainment, environmental monitoring, health care, manufacturing/industrial operations, retail, supply chain logistics, transportation, and others. Often included within the purview of IoT are a variety of “smart” applications, such as “Smart Homes,” “Smart Cities,” and “Smart Infrastructure.”²¹

This green paper will continue to use the term Internet of Things as an umbrella term to reference the technological development in which a greatly increasing number of devices are connected to one another and/or to the Internet. This acknowledges the widespread use and general popular acceptance of the term. The term itself is, as pointed out by some commenters, a misnomer, as many of the devices included in the Internet of Things do not use Internet Protocol or in any event may not connect directly to the Internet.²² At times, the IoT term is more descriptive of the system or network than an actual thing. IoT has become the commonly used term for the technologies and related issues discussed here, and for the sake of simplicity it will be used throughout this paper.²³

While this paper takes a broad, flexible approach to the definition of IoT, the Department understands that, in some contexts, a consensus technical definition may facilitate policy development and provide value to stakeholders. However, given the large diversity of devices, applications, and technologies captured under the umbrella of IoT, the Department will consider narrowly tailoring its policy inquiries and actions around categories of uses and/or devices rather than on all of IoT.

In the Request for Comment, the Department asked whether IoT should be treated as a single, unified subject or as a collection of specific categories, such as consumer IoT and industrial IoT. Many commenters supported categorizing IoT, particularly regarding concerns over policy issues such as privacy and safety.²⁴ Commenters pointed out that “industrial IoT,” for example, will usually not raise the same privacy concerns as connected consumer devices.²⁵ Similarly, the cybersecurity requirements necessary for medical devices may not be the same as the cybersecurity requirements for a stereo system.²⁶ Smart cities merit particular policy attention

²¹ Daniel Castro and Jordan Misra, “The Internet of Things,” Center for Data Innovation (November 2013), <http://www2.datainnovation.org/2013-internet-of-things.pdf>.

²² Kayleen Manwaring and Roger Clarke, Surfing the Third Wave of Computing: A Framework for Research into E-Objects, *Computer Law & Security Review* 31 (2015) 595.

²³ In this, IoT is similar to “big data,” in that the conversations and reports that were sparked by the popularity of the term were and continue to be important, while the term itself is less useful in laying distinct lines around particular technologies, functionalities, or the creation of specific procurement strategies. (*See generally*, Executive Office of the President, *Big Data: Seizing Opportunities, Preserving Values*, [May 2014].)

²⁴ *See, e.g.*, Association for Computing Machinery U.S. Public Policy Council Comment at 3; CompTIA Comment at 5-6; State of Illinois Comment at 20; Bugcrowd Comment at 3; Motorola Solutions Comment at 5.

²⁵ *See* Secure ID Coalition Comment at 2; BSA | The Software Alliance Comment at 5; Center for Data Innovation Comment at 11-12.

²⁶ Cisco Systems Comment at 25.

due to the investment and cooperation required to help communities realize the benefits of connectivity.²⁷ Automated or connected vehicles, unmanned aerial systems, and other types of connected devices also require specific, targeted attention due to the unique challenges and requirements that they pose to traditional regulatory frameworks.²⁸

The Department recognizes the importance of the missions of other federal agencies in responding to the challenges raised by IoT use in their areas of focus, and applauds the efforts made thus far to meet them. In the event that our terminology differs from that of other agencies, it may be that the differing terminology is appropriate given the context.

C. Benefits of IoT

From baby monitors to automatic climate control, IoT technologies promise a wide array of safety and efficiency benefits for consumers and businesses alike. While consumer-facing devices – such as exercise trackers, health monitors, and home safety systems – have drawn much of the media attention, Ligado Networks suggested that the most significant value for the U.S. economy is likely to result from enterprise IoT applications, particularly those that focus on industries such as manufacturing, agriculture, and infrastructure.²⁹ Broken down by industry, the manufacturing sector appears to have the most to gain from the adoption of IoT, with connected factories increasing productivity, optimizing inventory planning, reducing waste, and saving on energy costs and equipment maintenance. Industry is already exploring how connected devices can improve the safety and reliability of complex processes, and can achieve greater energy and operational efficiencies.³⁰

Connected devices are becoming a key tool for providing improved information about supply chains, distribution centers, land, and seaports; for tracking environmental and causal factors; and for helping to secure indoor and outdoor facilities. IoT technology can also help companies reimagine their supply chains, identifying inefficiencies or shipping delays, or confirming product integrity from manufacturing plant to a retail store.³¹ These devices are also prevalent in process-driven tasks in which instantaneous feedback and control are essential, such as in the energy sector. Businesses can use this improved data to eliminate inefficiencies in industries such as manufacturing, health care, transportation, energy, and retail.³²

²⁷ Executive Office of the President, Fact Sheet: Administration Announces New “Smart Cities” Initiative to Help Communities Tackle Local Challenges and Improve City Services (September 14, 2015), <https://www.whitehouse.gov/the-press-office/2015/09/14/fact-sheet-administration-announces-new-smart-cities-initiative-help>.

²⁸ Association of Global Automakers Comment at 3; AT&T Services Comment at 8.

²⁹ Ligado Networks Comment at 15.

³⁰ Providence Group Comment at 2.

³¹ Verizon Comment at 9; Georgia Institute of Technology, Center for Advanced Communications Policy and Rehabilitation Engineering Research Center for Wireless Technologies Comment at 3.

³² Zebra Technologies Comment at 10-11; Southern Company Services Comment at 1-2.

IoT technologies will generate data that helps companies make more-informed decisions, which in turn can improve efficiency, productivity, management, and quality control, regardless of the industry. For example, during transcontinental flights, the sensors on a commercial aircraft's various systems can generate data to improve safety and flight handling.³³ Telematic sensors in tens of thousands of delivery vehicles track engine performance, improve routing, and reduce fuel consumption and overall emissions.³⁴ Operators in a manufacturing facility with robotic assembly lines can automatically track every action down to the number of times a screw is turned. Any problems can be addressed as they are detected, which minimizes the impact on production.

Consumers are likely to see benefits from IoT in their homes. The Consumer Technology Association suggested that from the consumer perspective, Internet-enabled appliances, home automation components, and energy management devices are moving us toward a vision of the “smart home,” offering more security, energy efficiency, and convenience.³⁵ As the Alliance of Automobile Manufacturers noted in its comments, advancements in vehicle sensors, communications technology, and vehicle automation have the potential to significantly reduce the occurrence or severity of crashes by helping correct for errors in human driving.³⁶

Wearable fitness and health monitoring devices and network-enabled medical devices are expected to transform health care, according to the Direct Marketing Association.³⁷ Through remote health and education services, IoT technology holds immense promise for disadvantaged and rural communities. Connecting medical devices could greatly improve the quality and effectiveness of service, while also expanding the reach of medical professionals and reducing costs. For example, the GSM Association suggested that IoT-enabled remote health monitoring allows medical professionals to facilitate early interventions, improve adherence to medical regimes, and reduce readmission rates.³⁸ The Internet Society stated that IoT will be beneficial for people with disabilities and the elderly, improving levels of independence and quality of life at a reasonable cost by reducing the number of in-person visits needed to provide the required care.³⁹

IoT benefits are not confined to the business and consumer world. Streamlined data and analysis will also enable governments to deliver better, cheaper, and more efficient public services. The improvements suggested in emergency response and first responder capabilities alone are highly encouraging, such as increased collection and sharing of data among first responders. Further, many IoT infrastructure improvements have the ability to provide governments with cross-

³³ BSA | The Software Alliance Comment at 4.

³⁴ *Id.* at 4.

³⁵ Consumer Technology Association Comment at 3; National Association of Realtors Comment at 1.

³⁶ Alliance of Automobile Manufacturers Comment at 5; Future of Privacy Forum Comment at 5, 18.

³⁷ Direct Marketing Association Comment at 2.

³⁸ GSM Association Comment at 18.

³⁹ Internet Society Comment at 8.

cutting solutions. For example, according to the Future of Privacy Forum, sensors on roads and in traffic signals can allow for dynamic toll pricing and traffic control to decrease congestion.⁴⁰ Additionally, the Forum noted, these automated sensors can turn street lights on and off based on street use, potentially reducing both energy consumption and electricity costs.⁴¹ Connected devices can pinpoint costly leaks in water pipes, identify overflowing storm drains that threaten to mix public water with sewage, or detect the area of a power outage quickly without relying on reports from human observers. These devices can also help residents better understand their power or water usage, which may spur them to conserve use and help decrease their utility costs.⁴²

Cross-cutting IoT infrastructure advancements have the ability to improve countless government services. From Wi-Fi-enabled trash cans that inform waste management services when they are full in order to increase route efficiency and decrease fuel consumption, to IoT-enabled hospitals and emergency vehicles that can reduce wait times for medical services. BSA | The Software Alliance forecast in its comment that these types of IoT “smart city” initiatives will have an economic impact of up to \$1.6 trillion per year by 2025.⁴³

A key function of government at all levels, according to the Internet Society, is also to provide for the safety and security of its citizens, and the potential benefits of a robust IoT environment to improve public safety are well documented across law enforcement, fire services, emergency medical services, and homeland and border security.⁴⁴ Wearable sensors, body cameras, drones, and Global Positioning System (GPS) trackers are a few examples of technologies being deployed in the field today. Such devices will increase situational awareness to save lives, improve operational efficiency to lower costs, and enable predictive analytics to identify future public safety situations. Additionally, the proliferation of sensors and predictive analytics used by public safety practitioners will benefit citizens by providing real-time access to better information before disaster strikes, which will help people stay safe in emergencies.

D. Role of Government in Fostering IoT

The goal of this paper is to identify elements of an approach for the Department of Commerce to foster advancement of the Internet of Things, and defers to future policy makers to determine the value of crafting a national strategy. The paper – based on the record of comments received – reviews a range of issues and seeks to set out an approach that should be considered in any future discussions related to a national IoT strategy. According to commenters, any future national

⁴⁰ Future of Privacy Forum Comment at 16.

⁴¹ Consumer Technology Association Comment at 3.

⁴² See Infineon Technologies Americas Comment at 1-2; CTIA Comment at 3-4.

⁴³ BSA | The Software Alliance Comment at 4 (citations omitted).

⁴⁴ Internet Society Comment at 56; Jillisa Bronfman, *Weathering the Nest: Privacy Implications of Home Monitoring for the Aging American Population*, 208; National Emergency Number Association, National Association of State 9-1-1 Administrators Comment at 2.

strategy, if created, should strive toward global consistency and predictability and be based upon robust interagency coordination, public-private collaboration, and international engagement.⁴⁵

The U.S. Government, through numerous administrations, has a long record of promoting technology and innovation, and the Department expects to build on that foundation in our approach to the IoT environment. Dating back at least to the 1997 Framework for Global Electronic Commerce, the U.S. Government has been operating under the principle that the private sector should lead in digital technology advancement.⁴⁶ Even where collective action is necessary, the U.S. Government has encouraged multistakeholder approaches and private sector coordination and leadership where possible. When governmental involvement is needed, it should support and enforce a predictable, minimalist, consistent, and simple legal environment for commerce.⁴⁷ The Bush Administration, in its National Strategy to Secure Cyberspace (2003), affirmed the policy that the private sector and government must work together through a voluntary, collaborative process to protect the nation's connected infrastructure.⁴⁸

The U.S. Government has long recognized that innovation can drive economic growth and address national priorities through novel applications of new technologies.⁴⁹ The U.S. Government remains committed to the Principles for Internet Policy Making, adopted by the Organization for Economic Cooperation and Development (OECD) in 2011 that stress a flexible, multistakeholder approach to Internet policy making.⁵⁰ As the 2011 International Strategy for Cyberspace noted, "connectivity is no end unto itself; it must be supported by a cyberspace that is open to innovation, interoperable the world over, secure enough to earn people's trust, and reliable enough to support their work."⁵¹ Those concepts remain critical to our mission.

Commenters have urged the U.S. Government to avoid over-regulation that could stifle IoT innovation.⁵² The risk of premature and excessive regulation is notable given the size of the potential economic benefits to U.S. producers and consumers. Importantly, the U.S.

⁴⁵ Trans-Atlantic Business Council Comment at 4; Center for Data Innovation Comment at 26; Semiconductor Industry Association Comment at 11; Rapid7 Comment at 12.

⁴⁶ The Framework for Global Electronic Commerce (July 1997), <https://clinton4.nara.gov/WH/New/Commerce/>.

⁴⁷ Ibid.

⁴⁸ Executive Office of the President, National Strategy to Secure Cyberspace (February 2003), https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

⁴⁹ Executive Office of the President, A Strategy for American Innovation (October 2015), https://www.whitehouse.gov/sites/default/files/strategy_for_american_innovation_october_2015.pdf.

⁵⁰ OECD, OECD Principles for Internet Policy Making (2014), <https://www.oecd.org/sti/ieconomy/oecd-principles-for-internet-policy-making.pdf>

⁵¹ Executive Office of the President, International Strategy for Cyberspace (May 2011), 25, https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

⁵² Niskanen Center Comment at 9; Alliance of Automobile Manufacturers Comment at 9-10; U.S. Chamber of Commerce Center for Advanced Technology and Innovation Comment at 17.

Government's relevance is not only as a potential policymaker and regulator, but also as an enabler and adopter of IoT technology.⁵³

Several commenters called for a national strategy on IoT. As stated by the Center for Digital Innovation:

A national strategy for the Internet of Things, if designed and implemented correctly, would maximize the opportunity for the Internet of Things to deliver substantial social and economic benefits. The United States will not successfully capture these benefits by leaving development of the Internet of Things solely up to the market, just as no government actions could capture all of the potential benefits without a robust private sector that can innovate unencumbered by overly restrictive regulations.⁵⁴

The Semiconductor Industry Association commented that the “U.S. government should work with industry to establish a long-term national strategy that will enable America to lead the world in IoT ... that promotes key capabilities, including connectivity and interoperability, scalability and security, and complex intelligent analytics.”⁵⁵ Rapid7 called for “a national strategy with a set of overarching, high-level, voluntary principles generally accepted by government agencies and industry, which IoT security guidelines should follow ... [and can] enhance coordination and give agencies, regulated entities, and consumers a roadmap to incentivize development, awareness, and adoption of IoT security standards.”⁵⁶

Although no commenters opposed a national strategy, one cautioned that an overly prescriptive technology policy such as that seen in some parts of Asia and Europe could actually disadvantage American competitors as they seek to sell their IoT products worldwide.⁵⁷ The GSM Association urged the U.S. Government to focus on spurring IoT adoption and filling gaps that might hinder deployment if left entirely to market forces.⁵⁸

i. International Engagement

Those who commented on international engagement expressed the critical importance of a global free and open Internet to future innovation and growth in the IoT space.⁵⁹ On IoT issues internationally, the U.S. Government will need to maintain its robust advocacy for industry-led approaches and consensus-based standards and continue to use multistakeholder approaches to

⁵³ Trans-Atlantic Business Council Comment at 4.

⁵⁴ Center for Data Innovation Comment at 26.

⁵⁵ Semiconductor Industry Association Comment at 1.

⁵⁶ Rapid7 Comment at 12.

⁵⁷ *Id.* at 12.

⁵⁸ GSM Association Comment at 7.

⁵⁹ Internet Architecture Board Comment at 4; Computer & Communications Industry Association Comment at 6; Center for Data Innovation Comment at 23-24.

address policy challenges. Comments encouraging international engagements fell across a continuum of activities, including engagements focused on breaking down trade barriers, ensuring a consistent approach and common policy approach, and establishing formal IoT dialogues with interested parties.⁶⁰ The U.S. Government already has several formal government-to-government dialogues with some of our top trading partners that include digital economy issues. Within these existing dialogues, stakeholders commonly discuss issues such as cross-border data flows, technical standards, privacy, cybersecurity, spectrum allocation, IPv6, and cloud computing. The Department of Commerce expects IoT and related issues to be on the agenda of these international dialogues, and will support continued IoT engagement internationally, through various fora.

There is a wide variety of regional and international entities engaged in standards development related to IoT whose work, and work methods, are critical to the successful implementation of IoT policies. The Department will continue to support U.S. industry initiatives and participation in a range of standards bodies, and will actively advocate for work methods that recognize the value of private sector standardization efforts, and will continue to support greater collaboration between standards organizations. The Department will also advocate against attempts by governments to impose top-down, technology-specific “solutions” to IoT standardization needs.

The effects of varying policies and practices of countries around the world relating to IoT will almost certainly impact U.S. industry competitiveness. The Department of Commerce is aware that several governments recently released national policies and strategies related to the development of IoT. Regardless of whether the U.S. adopts an IoT national strategy, the government plays an important role in articulating and encouraging an approach to IoT policy and standards development worldwide that promotes a globally connected, open, and interoperable IoT environment.

ii. Stakeholder-Driven Policy Processes

In addition to its role advocating internationally for policies that are conducive to IoT advancement and balanced global policy, some commenters also noted that the U.S. Government can continue to play a role in convening public-private processes to address policy challenges in the IoT arena. Commenters acknowledged the success of the Department’s efforts to engage with stakeholders, including civil society and the private sector, in building flexible and adaptable frameworks, codes of conduct, and best practices in the fast-moving technology policy space.⁶¹ Examples include the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the Multistakeholder Forum on the Digital Millennium Copyright Act (DMCA)

⁶⁰ Microsoft Comment at 16; Symantec Comment at 5; U.S. Council for International Business Comment at 7.

⁶¹ CA Technologies Comment at 5; Family Online Safety Institute Comment at 4-5; CTIA Comment at 16; Internet Commerce Coalition Comment at 1, 4; Software & Information Industry Association Comment at 7; Cisco Systems Comment at 1, 13; AT&T Services Comment at 4, 28-9.

Notice and Takedown System, convened by the U.S. Patent and Trademark Office (USPTO) and the National Telecommunications and Information Administration (NTIA).⁶² Commenters noted that the U.S. Government should continue to employ these processes to solve policy challenges as an alternative to pursuing top-down regulatory solutions while IoT technologies are still advancing and gaining market scale.⁶³

3. An Approach for Departmental Action to Advance the Internet of Things

Given the great economic and social potential of IoT, as well as the qualitatively different challenges raised by its development, it is important for the Department to engage proactively yet selectively on issues described in this paper.

The Department has a longstanding approach to encouraging innovation in new technologies, while taking steps to address policy matters in a proactive, multistakeholder manner. We have approached emerging market trends and technologies with restraint and an eye toward allowing new entrants room to experiment and mature before they encounter significant government intervention. These guiding principles worked well as the Internet developed, and – as gleaned from our commenters – are appropriate to apply in the IoT sphere as well. Coupled with close partnership and collaboration with stakeholders, including our government and international partners, a cautious but thoughtful approach will map well to an emerging landscape where existing and new policy and technology norms and standards are starting to coalesce or collide. The overarching goal will remain the same: to foster the benefits of IoT while meeting its challenges.

Figure 1. The Department of Commerce will work across multiple stakeholder communities to foster IoT advancement.



⁶² See NIST, Framework for Improving Critical Infrastructure Cybersecurity, <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>. For information on the Forum, see <https://www.uspto.gov/learning-and-resources/ip-policy/copyright/multistakeholder-forum-dmca-notice-and-takedown-system>.

⁶³ See ADP Comment at 3; General Motors Comment at 3; U.S. Chamber of Commerce Center for Advanced Technology and Innovation Comment at 3-4.

Several principles – derived from stakeholder input – will guide the Department’s intended ongoing engagement with all stakeholders at the local, tribal, state, federal, and international levels across the evolving IoT landscape.

- ❖ The Department will lead efforts to ensure the IoT environment **is inclusive and widely accessible** to consumers, workers, and businesses;
- ❖ The Department will recommend policy and take action to support a **stable, secure, and trustworthy** IoT environment;
- ❖ The Department will advocate for and defend a **globally connected, open, and interoperable** IoT environment built upon industry-driven, consensus-based standards; and
- ❖ The Department will encourage IoT **growth and innovation** by encouraging expanding markets and reducing barriers to entry, and by convening stakeholders to address public policy challenges.

We have identified four broad areas of engagement:

- **Enabling Infrastructure Availability and Access:** Fostering the physical and spectrum-related assets needed to support IoT growth and advancement.
- **Crafting Balanced Policy and Building Coalitions:** Removing barriers and encouraging coordination and collaboration; influencing, analyzing, devising, and promoting norms and practices that will protect IoT users while encouraging growth, advancement, and applicability of IoT technologies.
- **Promoting Standards and Technology Advancement:** Ensuring that the necessary technical standards are developed and in place to support global IoT interoperability and that the technical applications and devices to support IoT continue to advance.
- **Encouraging Markets:** Promoting the advancement of IoT through Department usage, application, iterative enhancement, and novel usage of the technologies; and translating the economic benefits and opportunities of IoT to foreign partners.

We expect to work on a set of cross-cutting issues across these contexts from cybersecurity and privacy to innovation and intellectual property, with all stakeholders, at the local, tribal, state, federal, and international levels. The next section delves in depth into each of these areas of engagement, summarizing commenter feedback, describing current Department initiatives, and proposing next steps.

4. Areas of Engagement

As detailed below, the Department plans to work on IoT matters – with both ongoing and new activities – across a range of contexts.

A. Enabling Infrastructure Availability and Access

The expected increase in connected devices associated with IoT will dramatically increase demands upon the nation’s information and communications infrastructure.⁶⁴ It could put stress on legacy networks as well as more recently deployed all-Internet Protocol systems.⁶⁵

i. Increased Infrastructure Demand

IoT will depend upon both public and private communications networks, and will use various wireline and wireless modes, including satellite, often in combination or on an interdependent basis.⁶⁶ For example, different network resources may be used for access or backhaul, or to off-load traffic. The need for seamless connectivity will require deployment of robust broadband infrastructure for interconnecting devices.⁶⁷ Cisco estimates that, in addition to the anticipated expansion in the number of devices, Internet traffic will be 22 times greater in 2018 than 2013.⁶⁸ Such traffic growth is likely to dictate the need for greater overall network capacity – and smarter use of the bandwidth that is available.

Meeting these connectivity demands will require continued modernization of legacy telecommunications infrastructure and buildout of additional broadband capable networks. A percentage of the current telecommunications networks were primarily built for voice service and historically were largely copper-based. Over time, however, the demand for other services, including broadband Internet access, and more recently, video applications, has helped to fuel a transition to all-Internet Protocol-based multimedia networks using a variety of technologies such as fiber, hybrid fiber-coaxial cable, enhanced copper, and wireless networks that offer increased capacities. This transformation is allowing for much more dynamic, more efficient, and faster means of connecting devices. As a result, ongoing and future efforts across the country to spur increased broadband deployment and adoption should have a positive multiplier effect on IoT usage and functionality. Commenters did express concerns regarding hurdles to deploying infrastructure, including difficulties in siting of wireless towers and antennas, and access to

⁶⁴ See Competitive Carriers Association Comment at 2-3; Mobile Future Comment at 1.

⁶⁵ University Corporation for Advanced Internet Development Comment at 11.

⁶⁶ Inmarsat Comment at 2; Ligado Networks Comment at 6; Satellite Industry Association Comment at 1-2; Hughes Network Systems Comment at 1.

⁶⁷ United States Telecom Association Comment at 3-4 (citations omitted).

⁶⁸ Cisco Systems Comment at 17.

necessary poles, conduits, and rights-of-way.⁶⁹ With wireless networks, these problems are exacerbated by emerging architectures that require significantly more infrastructure than legacy systems.

ii. Increased Spectrum Demand

Wireless technologies are likely to play a significant role in supporting many of the increasing numbers of connected devices being developed by IoT manufacturers. In addition to existing wireless resources, IoT applications will leverage exciting technological advances, such as those associated with 5th generation (5G) wireless technologies, innovative unlicensed use of spectrum, low-power connectivity protocols, and others. Many commenters, however, pointed out that a shortage of available spectrum could become a constraint on the growth of IoT.⁷⁰

IoT-associated demand for spectrum access is rapidly expanding, from consumer-focused applications, to industrial systems to increasing government use cases. For example, Qualcomm pointed out that automated vehicles, critical infrastructure management, remote medical procedures, and command and control communications for unmanned aerial vehicles and robotics may all use different spectrum bands.⁷¹ Hewlett Packard Enterprise similarly commented that the expected diversity in connected devices and applications means that the required data rates as well as the duration and persistence of transmissions will vary widely, meaning that spectrum needs will be very different depending on the device and application.⁷²

Some commenters asserted the need for dedicated spectrum to support connected automobiles.⁷³ Today, automobiles already rely on connectivity for safety, convenience, and entertainment features. This trend is expanding, highlighted by the development of autonomous vehicles, and multiple communications technologies are likely to play a role.

Spectrum will also play a key role in the ability of utilities to leverage IoT technologies, according to the Edison Electric Institute. It also noted that utilities seek dedicated spectrum for broadband communications to manage peak loads, maintain grid stability, and monitor and control millions of utility system devices.⁷⁴ Deere & Company observed that many IoT systems, including those in agriculture, rely on unimpaired location services. As a result, Deere urged that government spectrum policies continue to protect the GPS from harmful interference.⁷⁵

⁶⁹ Wireless Infrastructure Association Comment at 2; Mobile Future Comment at 16; IoT Policy Network Comment at 8.

⁷⁰ Competitive Carriers Association Comment at 16; Consumer Technology Association Comment at 9-10; Semiconductor Industry Association Comment at 2; Karim Farhat Comment at 2.

⁷¹ Qualcomm Comment at i.

⁷² Hewlett Packard Enterprise Comment at 3.

⁷³ See General Motors Comment at 8-9; Alliance of Automobile Manufacturers at 7-8.

⁷⁴ Edison Electric Institute Comment at 6.

⁷⁵ Deere & Company Comment at 8.

IoT devices and applications will rely on various wireless technologies in rapidly escalating numbers, and they will use a number of licensed and unlicensed spectrum bands. This will increase demands on already scarce wireless spectrum resources.⁷⁶

As a result, commenters generally agreed that the U.S. Government can advance IoT by ensuring that our limited spectrum resources are used effectively and efficiently.⁷⁷ Many suggested that access to additional spectrum will be needed to support IoT,⁷⁸ with support for a balance between licensed and unlicensed access.⁷⁹ Some indicated that specific spectrum bands should be identified that could support IoT with some flexibility in exactly how such spectrum is used.⁸⁰ Many other commenters, however, recommended the federal government instead maintain its overall approach of meeting increasing demand by continuing to make available a broad range of spectrum on a technology neutral, flexible-use basis.⁸¹ AT&T commented that, for licensed spectrum, the licensee can manage and employ the spectrum it controls in an optimized fashion for the mix of traffic types that it needs to support.⁸² It also stated that such flexible commercial spectrum allocations allow the evolving market and consumers to determine the highest and best use of the spectrum and affords an opportunity for innovative technologies to emerge.⁸³

Commenters noted that the wireless industry requires access to a broad range of frequencies across the lower, middle, and higher spectrum bands to support enhanced connectivity for consumer, enterprise, and other uses, including IoT.⁸⁴ Some commenters urged the U.S. Government to encourage policies that ensure competitive carriers and small providers have access to additional licensed spectrum.⁸⁵ Hewlett Packard Enterprises suggested that dynamic sharing mechanisms and spectrum access systems may hold great promise for unlocking access to spectrum, particularly in sub-1 GHz bands, adding that the lack of spectrum availability in these bands is a potential constraint on the growth of IoT.⁸⁶ The Wi-Fi Alliance echoed this call for unlicensed access to spectrum in lower frequency bands.⁸⁷

⁷⁶ IoT Policy Network Comment at 8; State of Illinois Comment at 15; the U.S. Chamber of Commerce Center for Advanced Technology and Innovation Comment at 9.

⁷⁷ CTIA Comment at 14; Mobile Future Comment at 2; Ligado Networks Comment at 9; U.S. Chamber of Commerce Center for Advanced Technology and Innovation Comment at 10.

⁷⁸ 5G Americas Comment at 6; Consumer Technology Association Comment at 9-10.

⁷⁹ Verizon Comment at 12-13.

⁸⁰ IEEE-USA Comment at 2; ARM Comment at 6-7; Hewlett Packard Enterprise Comment at 2.

⁸¹ CTIA Comment at 14; 5G Americas Comment at 5-6; CompTIA Comment at 2-3; Telecommunications Industry Association Comment at 8; Silver Spring Networks Comment at 2-3.

⁸² AT&T Services Comment at 34-35.

⁸³ CTIA Comment at 14; CompTIA Comment at 4.

⁸⁴ Ligado Networks Comment at 13; Qualcomm Comment at 14; T-Mobile USA Comment at 15.

⁸⁵ Competitive Carriers Association Comment at 4-5; Ligado Networks Comment at 20.

⁸⁶ Hewlett Packard Enterprise Comment at 2.

⁸⁷ Wi-Fi Alliance Comment at 7.

iii. Internet Protocol Version 6 Adoption

There is a growing demand for Internet connectivity in light of IoT. Many devices connect to the Internet via Internet Protocol addresses (IP addresses). The system most in use today – Internet Protocol version 4 (IPv4) – was created in the 1970s as the Internet’s first, large-scale addressing system, and it provided us with nearly 4.3 billion IP addresses. This number, however, is far less than what the ever-expanding network – and IoT – will demand. As one commenter noted, IPv4 is an “outdated version of the Internet Protocol” which “severely restricts the number of devices that can be connected to the Internet.”⁸⁸

In the 1990s, the Internet technical community provided a sustainable solution to this problem by creating IPv6, the next generation protocol. IPv6 offers a significantly expanded addressing space that can comfortably meet the growing demand for Internet connections and obviate the need for technologies used to prolong the life of IPv4. Compared with IPv4’s 4.3 billion possible addresses, IPv6 offers 340 trillion trillion trillion addresses.

Although IPv6 addresses are available and plentiful, the majority of the Internet has not made the transition from IPv4 to IPv6.⁸⁹ Thus, a key question is what incentives or policy approaches can help quicken the pace of IPv6 adoption, in order to create the optimal enabling environment for the sustainable growth of IoT.⁹⁰ Due in large part to IoT, billions of additional devices – from industrial sensors to home appliances and vehicles – will be connected to the Internet between now and 2025.⁹¹ Commenters point out that the expected increase in connected devices associated with IoT will dramatically increase demands upon the nation’s information and communications infrastructure,⁹² and that “only IPv6 will scale to the size expected for Internet communication.”⁹³

⁸⁸ Internet2 Comment at 2.

⁸⁹ Continued use of IPv4 is made possible through technologies like “Network Address Translation” (NAT), which can be used to stretch dwindling IPv4 resources by allowing several devices or Things to share one IP address. Some view these technologies as only a temporary fix for the unavoidable problem of “IPv4 exhaustion.” This is due in large part to the different costs associated with doing so, for example the purchasing of new hardware, or the time needed to train employees and plan deployment. For many, without an understanding of the opportunities that it provides and the ultimate necessity for its adoption, the day-to-day costs of running a business will take precedence over long-term investment in IPv6, which can require a multi-year planning and testing process. Moreover, with technologies like NAT, businesses can continue to defer IPv6 implementation. Finally, for those businesses that do not provide ICT services but depend on them – especially SMEs – IPv4 exhaustion might be a scantily understood or even unknown issue.

⁹⁰ NTIA put out a Request for Comment on developing initiatives to increase IPv6 adoption in August, 2016. See NTIA [Request for Comments on the Incentives, Benefits, Costs, and Challenges to IPv6 Implementation](https://www.ntia.doc.gov/federal-register-notice/2016/incentives-benefits-costs-and-challenges-ipv6-implementation-0) (18 August 2016), available at: <https://www.ntia.doc.gov/federal-register-notice/2016/incentives-benefits-costs-and-challenges-ipv6-implementation-0>.

⁹¹ ISOC, “The Internet of Things: An Overview” Comment at 23.

⁹² Competitive Carriers Association Comment at 2-3; Mobile Future Comment at 1.

⁹³ Internet Architecture Board Comment at 3.

At the same time, however, one comment noted that IPv6 implementation requires many considerations, including security concerns generated by the capabilities of devices connected to the network. “Unlike IPv4, which was relatively simple to implement, IPv6 is more complicated,” Krawetz, et al, noted. “Many IoT devices do not fully implement IPv6. These incomplete implementations are vulnerable to network attacks and malware.”⁹⁴ The capacity of hardware and software to support IPv6 is one of several considerations to take into account when deploying IPv6 services. Despite this challenge and others, the Internet Society stated, many experts believe that IPv6 is “the best connectivity option and will allow IoT to reach its potential.”⁹⁵ In support of this effort, the Department will continue to encourage the adoption of IPv6 through its ongoing efforts to enhance standards profiles, support measurement and testing infrastructures, and foster multistakeholder collaboration.

iv. Issues of Equity in IoT

Connected devices have the extraordinary potential to improve the health, economic, and personal welfare of underserved communities. Wearable devices can closely monitor a patient’s health, which is critical for certain illnesses. Health care providers can do this remotely, which helps rural patients or patients with mobility problems. Because of this, it is essential that government and the private sector work together to ensure that all Americans have an opportunity to reap the benefits brought by IoT.

While IoT has the ability to improve the lives of consumers and citizens, a lack of access to the Internet, and thus many IoT applications, could also make things worse for underserved communities. The Center for Data Innovation commented that if “the public sector does not implement policies to encourage equitable deployment, the Internet of Things could exacerbate existing inequalities by providing the benefits of data-driven decision making only to some, and placing already underserved communities at an even greater disadvantage.”⁹⁶ In general, the concern is the cumulative impact of inequality (e.g., economic status plus other factors), and how some consumers may be left out of the benefits of IoT. The growth in IoT device use and the resulting data analytics from their use has been significant, and government should be conscious of issues of social inclusion and equity.⁹⁷

v. Planned Activities

It is clear from commenters that infrastructure needs to be deployed, developed, and maintained to ensure that IoT reaches its full potential. This will require a continued focus on the deployment of, and investment, in wireline and wireless connectivity, spectrum availability, and

⁹⁴ Neal Krawetz, Eric Schultz, Valerie Kaminsky, Bill Tucker, et al. at 15

⁹⁵ Internet Society Comment at 27.

⁹⁶ Center for Data Innovation Comment at 7.

⁹⁷ White House, *Big Data: Seizing Opportunities, Preserving Values* (May 2014), https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf.

standards development. The push for infrastructure deployment and development should be private-sector led, with the support of the Department to assess spectrum requirements, promote and foster broadband deployment, and ensure that access is made available to all communities. IoT infrastructure development will also require international engagement to address issues of interoperability, access, and inclusiveness.

1. *Current Initiatives*

- **Empowering Communities to Become Smart Cities.** NTIA assists in the development of the broadband infrastructure necessary for the use of IoT both directly through toolkits and indirectly through work with the Broadband Opportunities Council (BOC). Private-sector partners can be an important source of capital, technical knowledge, continuing innovation, and workforce development. To assist communities looking to embed new digital technologies into municipal infrastructure, NTIA released *Using Partnerships to Power a Smart City: A Toolkit for Local Communities* for local officials and citizen groups to use as a guide for building successful public-private partnerships.⁹⁸ The Department co-chairs the BOC, which includes 25 federal agencies and departments and that engages with industry and other stakeholders to understand ways the Executive Branch can better support the needs of communities seeking broadband investment. The BOC released a report in September 2015 that includes action items and milestones for each agency, and will continue its work to monitor implementation of the action items and to explore additional steps that can be taken to remove barriers to broadband deployment and adoption.⁹⁹
- **Research and Development into Spectrum-Related Interactions.** NTIA's Institute for Telecommunication Sciences (ITS) is investigating interaction effects among new IoT-related spectrum use and incumbent spectrum users in cases where they are collocated and/or in adjacent bands. This is creating a technically neutral body of knowledge and expertise to inform future policy. Continued development of this IoT testbed will provide a better understanding of the performance and behavior of IoT systems. It will also establish a base of scientific principles to inform neutral and accurate predictions of future spectrum needs and trouble areas. Using the scientific principles derived by the continued development of the IoT testbed, ITS also plans to develop the capability to model large-scale interactions of currently deployed and new, not-yet deployed IoT systems.

⁹⁸ *Using Partnerships to Power a Smart City: A Toolkit for Local Communities*, https://www2.ntia.doc.gov/files/smartcities-toolkit_111516_v2.pdf.

⁹⁹ *Broadband Opportunity Council Report and Recommendations*, https://www.whitehouse.gov/sites/default/files/broadband_opportunity_council_report_final.pdf.

- Enabling IoT Functionality for First Responders.** An anticipated key driver of the benefits of IoT for public safety is the First Responder Network Authority's (FirstNet) Nationwide Public Safety Broadband Network (NPSBN). FirstNet is deploying the necessary infrastructure to allow for transfers of data wirelessly, real-time in the field, without potential congestion from commercial network traffic. This will be crucial during routine day-to-day incidents, large planned events or unexpected disasters. In 2012, Congress allocated \$7 billion and 20 megahertz of spectrum to FirstNet to partner with the private sector to build the NPSBN, an LTE-based wireless broadband network dedicated to public safety. Once operational, the FirstNet network promises to transform the way first responders communicate, providing public safety personnel with dedicated access over a prioritized, reliable, and secure mobile connection. This will enable first responders to send and receive text, voice, video, images, location information, and other data in real time to help increase situational awareness and operational capability in the field.

In addition to revolutionizing emergency communications, the FirstNet network will be an incubator and proving ground for public safety focused IoT solutions by linking more first responder data sources, such as their gear, emergency vehicles, fingerprint scanners, databases, and more. The constant transfer of data over a dedicated, mission critical network will enable faster decision making that can help coordinate responses and save lives. By focusing on public safety needs first, FirstNet seeks to drive industry to continue to innovate to improve public safety activity to save lives, improve responses to incidents and disasters, and better anticipate future responses.

- IPv6 Adoption.** The Department is championing IPv6 adoption and use in networks, devices, and websites, and promoting more IPv6-enabled content, but there is more to be done. NIST leads IPv6 planning within the U.S. Government, and developed the technical infrastructure to assist the Government with IPv6 adoption.¹⁰⁰ NTIA and NIST have in the past supported awareness-raising and information-sharing by holding public meetings on IPv6,¹⁰¹ and have produced informational resources to help those implementing the new protocol, including a *Technical and Economic Assessment of IPv6* (2006) and an *IPv6 Readiness Tool for Business* (2011).¹⁰² NIST leads IPv6 planning within the U.S. Government, and developed the technical infrastructure (i.e., standards profiles, testing infrastructure, and deployment guidance) to assist the government with

¹⁰⁰ See the NIST Information Technology Laboratory, Advanced Network Technologies Division website, available at <https://www-x.antd.nist.gov/usgv6/>.

¹⁰¹ NTIA and NIST have held two public workshops on IPv6 (2004, 2010), <https://www.ntia.doc.gov/federal-register-notice/2004/notice-public-meeting-ipv6>; <https://www.ntia.doc.gov/page/ipv6-workshop-09282010>.

¹⁰² These resources and more are available on NTIA's website, <https://www.ntia.doc.gov/page/additional-ipv6-resources>.

IPv6 adoption.¹⁰³ The agency also maintains up-to-date statistics on IPv6 deployment.¹⁰⁴ NTIA conducted a Request for Comment (RFC) on the *Incentives, Benefits, Costs and Challenges to IPv6 Implementation* in order to better understand the industry's experience with and viewpoints on IPv6 implementation, and received a number of high quality insights from individuals, cloud providers, Internet service providers, and various industry associations.¹⁰⁵

2. Proposed Next Steps

The Department will:

- Coordinate with the private sector, as well as federal, state, and local government partners, to ensure the infrastructure to support IoT continues to expand, that access to infrastructure is inclusive and affordable, and that the infrastructure remains innovative, open, secure, interoperable and stable. This includes promoting adoption and usage to encourage deployment and investment, and engaging in technical assistance and research and development.
- Continue to innovate in spectrum management to increase access to spectrum that will help facilitate IoT growth and advancement. NTIA, through its Office of Spectrum Management, will collaborate with stakeholders, including its spectrum-related interagency (Policy and Plans Steering Group and Interdepartmental Radio Advisory Committee) and external advisory bodies (Commerce Spectrum Management Advisory Committee), to assess the spectrum implications of the diverse IoT applications that currently or in the future may be delivered through a number of technologies operating in various spectrum bands.
- Expand its digital inclusion efforts to include an emphasis on IoT adoption and availability.
- Continue to encourage the adoption of IPv6 by fostering multistakeholder collaboration and dialogue and provide a platform for discussion on issues such as mobile IPv6 routing, security in dual-stack environments, and privacy implications of IPv6.

¹⁰³ See the NIST Information Technology Laboratory, Advanced Network Technologies Division website, available at <https://www-x.antd.nist.gov/usgv6/>.

¹⁰⁴ <https://usgv6-deploymon.antd.nist.gov/cgi-bin/generate-gov>.

¹⁰⁵ NTIA [Request for Comments on the Incentives, Benefits, Costs, and Challenges to IPv6 Implementation](https://www.ntia.doc.gov/federal-register-notice/2016/incentives-benefits-costs-and-challenges-ipv6-implementation-0) (18 August 2016), available at: <https://www.ntia.doc.gov/federal-register-notice/2016/incentives-benefits-costs-and-challenges-ipv6-implementation-0>.

- Collect data and conduct analysis on the usage and growth of IoT devices through its Digital Nation data collection in order to better inform industry and policy makers.

B. Crafting Balanced Policy and Building Coalitions

Commenters detailed several discrete policy areas that will require coordinated engagement by all stakeholders – government, civil society, academia, the technical community, and the private sector, globally and domestically – to ensure forward-looking, adaptable, and balanced policy that fosters innovation while addressing risks and challenges.

i. Cybersecurity

IoT will be integrated into our lives to an unprecedented degree. While the computer and Internet revolutions have pushed more of our lives into the data domain, IoT will continue that trend and bring both software and connectivity into almost every aspect of the home, enterprise, and public space. One comment noted that several factors contribute to the more challenging environment of increased connectivity, including: the highly networked nature of IoT creates a large number of attack surfaces that can be exploited; some IoT device makers have not followed established cybersecurity best practices used in other information security contexts; and some connected devices will collect vast amounts of personal information, enabling high impact attacks.¹⁰⁶

Meanwhile, the expected ubiquity of and dependence on IoT magnifies the security risk on each domain, whether it is the power grid, our automobiles, or children’s toys. The distributed denial of service (DDOS) attack in October 2016 on a Domain Name Service (DNS) provider’s lookup service that used an army of IoT devices protected only by factory-default passwords is an example of how Internet-connected devices have changed the cybersecurity environment.¹⁰⁷ The incident was the most visible and far-reaching example of the potential risks that must be mitigated when considering IoT. Incident management in cases such as these may require enhanced coordination by the private sector, government, and individuals in the future.

The risks for IoT systems that support the economy’s industrial sectors are even more challenging, according to IBM. Industrial devices are connected to the Internet to allow for broader visibility, control, and maintenance, but these devices can also become potential attack targets.¹⁰⁸

At the same time, commenters noted that cybersecurity best practices are a new concept for many IoT stakeholders. Mature manufacturers of newly wired devices, such as an appliance manufacturer developing a wireless-enabled refrigerator, may have little to no experience

¹⁰⁶ ABA Section of Science & Technology Law Comment at 11.

¹⁰⁷ Brian Krebs, Hacked Cameras, DVRs Powered Today’s Massive Internet Outage, Krebs on Security (October 21, 2016), <https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/>.

¹⁰⁸ IBM Comment at 5.

collecting, securing, and protecting consumer data, the Electronic Frontier Foundation (EFF) said in its comments.¹⁰⁹ EFF added that start-ups building IoT technologies and interfaces for the first time may focus primarily on getting a product to market, without considering how to protect and secure computer networks or data.¹¹⁰ Commenters stated that different sets of best practices will be relevant for different IoT entities, such as hardware manufacturers/integrators, developers, deployers, and operators.¹¹¹

1. *Need for Flexible, Risk-based Solutions*

Threats and vulnerabilities are constantly evolving. Predefined solutions quickly become obsolete or even provide bad actors with a roadmap for attack, the U.S. Chamber of Commerce noted.¹¹² Many commenters stated that regulators must allow developers the flexibility to create cutting-edge improvements to defend their products and services and protect their users.¹¹³ Overly prescriptive regulations could impede stakeholders' abilities to respond to ever-changing threats, AT&T commented.¹¹⁴ Cisco stated that governments should work within existing regulatory structures, and focus on outcome-oriented approaches to manage newly identified risks associated with the use of particular technologies, instead of regulating the underlying technologies.¹¹⁵

The U.S. Government can play a valuable role in driving awareness and resolution of the cybersecurity issues facing IoT development, Rapid7 wrote, suggesting the government can facilitate coordination and standardization among IoT stakeholders to improve security.¹¹⁶ Several commenters called for a greater recognition of the role played by the security research community, which can independently discover, assess, and correct cybersecurity vulnerabilities.¹¹⁷

Commenters recommended that the U.S. Government continue to foster a community for cybersecurity information sharing, and collaborate with industry on clearer guidelines for security research and coordinated disclosure.¹¹⁸ The Information Technology Industry Council pointed to two examples of public-private partnerships that can help ensure greater coordination

¹⁰⁹ Electronic Frontier Foundation Comment at 5.

¹¹⁰ *Ibid.*

¹¹¹ See Microsoft Comment at 7; Information Technology Industry Council Comment at 8; Software & Information Industry Association Comment at 2.

¹¹² U.S. Chamber of Commerce Center for Advanced Technology and Innovation Comment at 13.

¹¹³ See Application Developers Alliance Comment at 4; AT&T Services Comment at 45; Cisco Systems Comment at 22-23.

¹¹⁴ AT&T Services Comment at 45.

¹¹⁵ Cisco Systems Comment at 23.

¹¹⁶ Rapid7 Comment at 8-9.

¹¹⁷ See Access Now Comment at 8; Rapid7 Comment at 6; ACM U.S. Public Policy Council Comment at 5.

¹¹⁸ See IBM Comment at 14; Access Now Comment at 7; U.S. Chamber of Commerce Center for Advanced Technology and Innovation Comment at 14.

and collaboration across the government: information sharing and analysis centers and sector coordinating councils.¹¹⁹

Commenters suggested some limited areas that may require special consideration. Devices that are used by children may constitute one of these areas.¹²⁰ For example, as Common Sense Kids Action pointed out, a recent data breach involving a toy manufacturer exposed names, dates of birth, password recovery questions and answers, genders, pictures of parents and children, audio recordings of children, and chat logs between parents and children.¹²¹ Autonomous vehicles may be another area for special consideration, particularly regarding safety-critical systems. The Association of Global Automakers recommended Federal criminal penalties for those who electronically tamper with a motor vehicle without the owner's consent.¹²²

The range of IoT devices and applications, as well as the many potential attack vectors and harms, may preclude a single, prescriptive solution. Instead, many commenters advocated a risk-based approach to understand threats and vulnerabilities.¹²³ Just as there is no easy description for IoT itself, there is no single prescription for IoT security. Commenters argued that breaking down the security challenge into particular risks allows for a better understanding of the solution space. Symantec, for example, distinguishes between risks to communications to/from an IoT device, and risks that undermine the integrity of the device itself.¹²⁴ Many other commenters highlighted the fact that concerns about the risks to data confidentiality and integrity can be best addressed by encryption,¹²⁵ while other commenters said that concerns about the risk of malicious control of devices require access control and authorization mechanisms.¹²⁶ At the September 2016 IoT workshop, the Providence Group's Dan Caprio stated that IoT risk is such a complex and multifaceted issue that it needs to be addressed through an enterprise risk management approach.¹²⁷

This emphasis on a risk-based approach conforms with a broader focus across the Department on understanding and addressing cybersecurity risks in the business/mission context.¹²⁸ This

¹¹⁹ Information Technology Industry Council Comment at 9.

¹²⁰ See Family Online Safety Institute Comment at 3; Future of Privacy Forum Comment at 10; Common Sense Kids Action Comment at 2; Staff of the Federal Trade Commission's Bureau of Consumer Protection and Office of Policy Planning Comment at 6.

¹²¹ Common Sense Kids Action Comment at 2-3.

¹²² Association of Global Automakers Comment at 5.

¹²³ Infineon Technologies Americas Comment at 6; the U.S. Chamber of Commerce Center for Advanced Technology and Innovation Comment at 13; Software & Information Industry Association Comment at 9.

¹²⁴ Symantec, "An Internet of Things Reference Architecture" Comment at 2, 16.

¹²⁵ See Internet Association Comment at 6; Telecommunications Industry Association Comment at 13.

¹²⁶ See Rapid 7 Comment at 12; Samsung Comment (June 2, 2016) at 3.

¹²⁷ Fostering the Advancement of the Internet of Things Workshop, September 1, 2016, Transcript, <https://www.ntia.doc.gov/files/ntia/publications/09012016-iot-workshop.pdf>.

¹²⁸ Executive Office of the President, Executive Order – Improving Critical Infrastructure Cybersecurity, February 12, 2013, <https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>.

approach is embodied within the NIST Framework for Improving Critical Infrastructure Cybersecurity (NIST Framework). Many commenters referenced the NIST Framework as providing a model to think about cybersecurity for IoT applications and devices.¹²⁹ The NIST Framework offers an overarching structure to address cybersecurity across all critical infrastructure sectors using existing international standards and best practices, while providing adaptability and flexibility to meet the unique needs of each sector and address new threats.

The NIST Framework highlights the limitations of a “one-size-fits-all” solution and instead is a voluntary, flexible framework that can be scaled to organizations’ different needs, allowing them to take into account their particular business models, assets, and other variables. This structure enables organizations to adapt to an ever-changing, dynamic environment, which is critical for IoT technologies. Verizon called for a process expanding on NIST’s model that builds on collaboration between industry, academic, and government stakeholders to identify standards and practices for IoT security.¹³⁰

2. Security by Design

Many commenters underscored the importance of security considerations as an integral part of the entire life cycle of IoT products, from conception to deployment and beyond. The Software & Information Industry Association, for example, encouraged a practice of a risk assessment during the product design stage and security testing during development and before products and services launch.¹³¹ When integrating multiple components, Rapid7 suggested that each component must be understood well enough to configure it properly to minimize unused features and secure any insecure defaults.¹³²

As several commenters noted, a common means of capturing this holistic approach to security is “security by design,”¹³³ a concept the Department strongly supports.¹³⁴ This is not a new idea, and is linked to important concepts like “privacy-by-design.”¹³⁵ The Federal Trade Commission has also embraced this approach, with its IoT guidance that companies “Start with Security.”¹³⁶

¹²⁹ CTIA Comment at 16; CA Technologies Comment at 5; Coalition for Cybersecurity Policy & Law Comment at 4-5.

¹³⁰ Verizon Comment at 20.

¹³¹ Software & Information Industry Association Comment at 9.

¹³² Rapid7 Comment at 3-4.

¹³³ See, e.g., Software & Information Industry Association Comment at 9; Nest Labs Comment at 14; ARM Comment at 5.

¹³⁴ See remarks of Secretary Penny Pritzker at the U.S. Chamber of Commerce, September 27, 2016. “[A]t the National Telecommunications and Information Administration, we are engaging stakeholders in fast-growing sectors like the ‘Internet of Things’ to ensure that the cars, home security systems, baby monitors, and devices of the future are born secure.”

¹³⁵ Software & Information Industry Association Comment at 11; Thierer Comment at 90. For more, see NIST Privacy Engineering program at http://csrc.nist.gov/projects/privacy_engineering/.

¹³⁶ Federal Trade Commission, Start With Security: A Guide for Business (June 2015), <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

The overall notion is often most easily understood in its absence: security failures are more likely to occur when security is not a consideration throughout the concept and design process. Attempts to “bolt on” security features late in the product development process are both more expensive and more prone to error.

While many commenters embraced this notion, there is no clear consensus or straightforward path on how to implement such a concept across the broad IoT space. The software industry has spent many years developing tools, techniques, and standards for integrating security into the development lifecycle. These range from approaches developed by specific companies to those developed by open standards organizations.¹³⁷ The Information Technology Industry Council suggests starting at the hardware level with built-in safeguards.¹³⁸ Other mechanisms for building in security include considering authentication tools, using modern, well-tested software packages, and having a complete testing protocol in place. Designers, developers, and integrators must understand security from an initial stage. Further tools to empower easier security decision-making may be necessary as IoT grows.

The final hurdle to security-by-design is the challenge of how to communicate the effectiveness of security practices to customers, relevant regulators, and the public. This problem is not unique to IoT, but is necessary to foster public trust and market rewards for security investment.

3. Patching

The lifecycle of a device lasts beyond the development process and will vary greatly depending on the device, from short periods to many years. The Electronic Frontier Foundation noted that unpatched smart devices create security vulnerabilities and can put privacy at risk by making devices easier to compromise or by leaking user information.¹³⁹ Manufacturers of connected devices, unlike those who make traditional computers, often lack an effective update and upgrade path once the devices leave the manufacturer’s warehouse. Several commenters noted that, without a patching capability, it is difficult to mitigate devices’ known security flaws on a large scale.¹⁴⁰ These vulnerabilities can have potentially devastating consequences for users.¹⁴¹

Many manufacturers entering the IoT space do not traditionally offer frequent or fast-paced support or updates to their products, and are only beginning to look into quick response practices

¹³⁷ See, e.g., Microsoft (<https://www.microsoft.com/en-us/sdl/>); Building Security in Maturity Model (<https://www.bsimm.com/about/>); Software Assurance Maturity Model (https://www.owasp.org/index.php/OWASP_SAMM_Project); NIST Special Publication 800-160 (http://csrc.nist.gov/publications/drafts/800-160/sp800_160_second-draft.pdf); ISO/IEC 27034:2011 (<http://www.iso27001security.com/html/27034.html>).

¹³⁸ Information Technology Industry Council Comment at 7.

¹³⁹ Electronic Frontier Foundation Comment at 5.

¹⁴⁰ See Software & Information Industry Association Comment at 9; Coalition for Cybersecurity Policy & Law Comment at 5; Internet Architecture Board Comment at 3; Rapid7 Comment at 3.

¹⁴¹ Comment of Association for Computing Machinery, ACM U.S. Public Policy Council at 6.

for vulnerability patching, Rapid7 commented.¹⁴² Effective patching is challenging even for mature market sectors that have update mechanisms, such as smartphones and routers, and therefore Rapid7 suggests IoT newcomers will need to quickly incorporate patching and updating processes into their practices.¹⁴³

Many connected devices are likely to be long-lived (sometimes lasting decades), and many will undoubtedly require patches as security issues are identified in the future. For example, cars are purchased with the expectation that they will be used for at least 11 years.¹⁴⁴ Commenters suggested that methods to allow updates from reputable sources, sometimes despite low bandwidth and intermittent connections especially over the long term, should be considered. This is important even if the original manufacturer or service provider no longer supports the device or is no longer in business.¹⁴⁵ Meanwhile, Microsoft pointed out that many connected devices will be deployed into environments that fall under multiple jurisdictions with different regulatory requirements, or into consumer environments with fewer security management resources.¹⁴⁶

4. Technical Limitations

One comment highlighted the technical limitations of many IoT devices as a particular hurdle for implementing known good security practices.¹⁴⁷ These limitations include computationally weak hardware, minimal operating systems, and/or limited memory, commented Krawetz et al. They added that limited resources make connected devices more vulnerable to denial of service and stacksmashing attacks (causing a stack in a computer application or operating system to overflow, which may subvert or crash the stack); the IoT world has not yet developed common mitigation techniques.¹⁴⁸ Even when adequate technology exists, devices may lack the metrics or interfaces for security awareness. CTIA commented that a breach could exist for an extended period of time before being noticed, and once noticed, correction or mitigation may not be possible or practical.¹⁴⁹ Alternative solutions may require greater coordination across different parts of the IoT environment.

The difficulties and costs of implementing encryption on technically limited devices drew substantial comment. Researchers who studied IoT encryption found that many of the devices

¹⁴² Rapid7 Comment at 3.

¹⁴³ Id.

¹⁴⁴ See <http://www.consumerreports.org/cro/2012/05/make-your-car-last-200-000-miles/index.htm>

¹⁴⁵ See Association for Computing Machinery, ACM US Public Policy Council Comment at 6; Consumer Federation of America Comment at 5; Neal Krawetz et al. Comment at 5-6; Coalition for Cybersecurity Policy & Law Comment at 5.

¹⁴⁶ Microsoft Comment at 7.

¹⁴⁷ Jillisa Bronfman Comment at 223.

¹⁴⁸ Neal Krawetz et al. Comment at 12.

¹⁴⁹ CTIA Comment at 18 (citations omitted).

exchanged completely unencrypted information with servers.¹⁵⁰ Even devices that did encrypt the data traffic they sent and received were at times revealing other points of information, such as when power had been turned on or off.¹⁵¹ Many commenters agreed that encryption is important in all areas of the IoT environment, including at the device level, for data in transit, and at the platform or service level. Commenters urged the government to encourage the adoption and use of the best commercial encryption implementations and security practices available.¹⁵²

While encryption is just one of many important capabilities, it drew numerous comments. The Niskanen Center stated that strong encryption has significant economic benefits, encouraging and promoting the trust necessary for robust online commerce and finance.¹⁵³ NIST has already begun to explore the potential of “lightweight encryption” for devices with low computing power.¹⁵⁴

ii. Privacy

Potential privacy concerns arising from the use of IoT devices were second only to cybersecurity in number of comments received. While it is clear that consumer trust is essential to the growth of IoT,¹⁵⁵ and that ensuring the privacy of users is a key aspect of building that trust, commenters were divided on whether IoT presents novel privacy challenges and on the appropriate response to these challenges.

It is clear that connected devices are not all equal in their relative effects on privacy. According to some commenters, industrial, agricultural, and other non-consumer facing uses of IoT generally would not likely collect information that could be considered personally identifiable information.¹⁵⁶ Any policy response to privacy concerns would need to avoid placing regulatory burdens on applications that pose limited potential for privacy-related harms. There is also a danger in creating too many “sector-specific” regulatory requirements. For example, the GSM Association stated that “privacy considerations that accompany IoT will affect different sectors of the economy, and conflicting, sector-specific regulations will hinder IoT development and

¹⁵⁰ Electronic Privacy Information Center Comment at 7 (citations and internal quotations omitted; emphasis original).

¹⁵¹ Nick Feamster, *Who Will Secure the Internet of Things?*, Freedom to Tinker (Jan. 19, 2016), <https://freedom-to-tinker.com/blog/feamster/who-will-secure-the-Internet-of-things/> (emphasis in original).

¹⁵² See Computer & Communications Industry Association Comment at 10-11; ACT | The App Association Comment at 4; BSA | The Software Alliance Comment at 5.

¹⁵³ Niskanen Center Comment at 6.

¹⁵⁴ Draft NISTIR 8114 Report on Lightweight Cryptography (August 2016), http://csrc.nist.gov/publications/drafts/nistir-8114/nistir_8114_draft.pdf.

¹⁵⁵ Alain Louchez Comment at 6.

¹⁵⁶ GSM Association Comment at 8; Center for Data Innovation at 11. Such uses may implicate business confidential information and/or trade secret issues, see *infra* Section 3.G.iii (discussing trade secrets).

deployment.”¹⁵⁷ Many commenters nonetheless argued for a “privacy-by-design” approach,¹⁵⁸ or the use of privacy enhancing technologies (PETs).¹⁵⁹ These techniques would typically need to be implemented before the developers determine the use for devices or components that are deployed in both consumer-facing and non-consumer facing applications.

Several commenters argued that there are no new privacy issues related to IoT,¹⁶⁰ that it is too early to craft regulatory responses,¹⁶¹ or that current regulation is sufficient.¹⁶² The U.S. Chamber of Commerce stated that “[w]ithout evidence of heightened privacy concerns or consumer harm, there is no reason not to allow the IoT market to mature under the frameworks that exist for protecting consumers’ legitimate privacy interests.”¹⁶³ These commenters primarily pointed to Federal Trade Commission enforcement of its Section 5 authority over unfair or deceptive practices, sector-specific legislation such as the Children’s Online Privacy Protection Act, and the Health Insurance Portability and Accountability Act as providing the protections needed by consumers.¹⁶⁴ Verizon, for example, stated that “[p]olicymakers should leverage existing privacy frameworks – including the existing Federal Trade Commission regime and self-regulatory mechanism – to create a holistic policy approach to IoT-related privacy issues. Doing so will create the necessary regulatory certainty and stability to support continued investment and growth in IoT solutions.”¹⁶⁵ These commenters are concerned about the potentially negative effect that proactive regulation would have on innovation and growth in IoT.¹⁶⁶

Other commenters argued that the privacy concerns raised by IoT were either novel¹⁶⁷ or were different enough in scale, scope, and stakes to necessitate distinct consideration.¹⁶⁸ As Microsoft argued, “IoT raises unique privacy concerns. IoT will dramatically increase the number of devices facilitating the creation, collection and transmission of data. In parallel, connected devices without screens or other direct user interfaces create significant practical challenges for privacy regimes based primarily on notice and consent.”¹⁶⁹

¹⁵⁷ GSM Association Comment at 16.

¹⁵⁸ Cisco Systems Comment at 24; Jillisa Bronfman Comment at 220; Verizon Comment at 19.

¹⁵⁹ Electronic Privacy Information Center Comment at 11.

¹⁶⁰ See Computer & Communications Industry Association Comment at 4; Center for Data Innovation Comment at 6.

¹⁶¹ See Niskanen Center Comment at 5; National Cable & Telecommunications Association Comment at 6; U.S. Chamber of Commerce Center for Advanced Technology and Innovation Comment at 3.

¹⁶² See U.S. Chamber of Commerce Center for Advanced Technology and Innovation Comment at 11; CompTIA Comment at 5; NetChoice Comment at 2-3.

¹⁶³ U.S. Chamber of Commerce Center for Advanced Technology and Innovation Comment at 11.

¹⁶⁴ See Nest Labs Comment at 8-10.

¹⁶⁵ Verizon Comment at 17.

¹⁶⁶ Consumer Technology Association Comment at 16; General Motors Comment at 5.

¹⁶⁷ See Microsoft Comment at 10; Open Connectivity Foundation Comment at 6; Public Knowledge Comment at 13; ACM US Public Policy Council Comment at 6-7.

¹⁶⁸ See Symantec Comment at 1; Sysorex USA Comment at 3.

¹⁶⁹ Microsoft Comment at 10.

Commenters also raised the challenge of notice and consent, suggesting the need for flexibility and modernization of how consent is gained.¹⁷⁰ Given the vast amounts of data that IoT devices are capable of collecting, commenters also discussed the link between the privacy concerns raised by IoT and those inherent in the discussions of big data,¹⁷¹ with the paramount concern being the need to combat potential discrimination, secure collected data, and promote transparent decision-making processes. Symantec states:

The unprecedented volume of data that will be generated by connected devices will in many applications raise significant privacy issues. First and most obviously, an exponential increase in data collection brings with it a similar increase in the potential for and damage from a data breach. This data will need to be securely collected, transmitted, and stored. But the analytics that can be applied to all of this data raises different issues, as Americans are increasingly concerned with how big data is providing corporations and governments insight into their lives. As with security, the first step towards addressing these issues is transparency – people should have the opportunity to understand how data about them is being secured, just as they should know how that data is being used.¹⁷²

Many commenters expressed significant concern about the ubiquity of data collection and the potentially sensitive or personal nature of this data. The Electronic Frontier Foundation cited a Hewlett Packard Enterprise study that “found that 90 percent of IoT devices collected at least one piece of personal information via the device, the cloud, or its mobile application.”¹⁷³ At the September 2016 IoT workshop, Michelle De Mooy of the Center for Democracy and Technology stated that these concerns are intertwined with concerns about security, given that insecure data is the primary way in which user privacy is likely to be breached. Straddling the line between privacy and security concerns is the need to address data breach notification policy, which is currently a patchwork of laws and regulations.¹⁷⁴ Commenters also raised the need to address the problem of data ownership over the lifecycle of a consumer device.¹⁷⁵

The scope of personal data collected by connected devices is potentially immense, expanding far beyond the usual concerns of traditional e-commerce. The systematic collection of personal information, habits, locations, and physical conditions over time can easily allow an entity that has not directly collected this information to infer specific details about the user or users of the

¹⁷⁰ Microsoft Comment at 2; Future of Privacy Forum Comment at 9; Kim L. Jones Comment at 2.

¹⁷¹ Cisco Systems Comment at 26-27; Hewlett Packard Enterprise Comment at 5.

¹⁷² Symantec Comment at 4.

¹⁷³ Electronic Frontier Foundation Comment at 2.

¹⁷⁴ CompTIA Comment at 5; Access Now Comment at 4.

¹⁷⁵ See Symantec Comment at 2-3; Staff of the Federal Trade Commission’s Bureau of Consumer Protection and Office of Policy Planning Comment at 9; Verizon Comment at 21. This also has intellectual property implications as discussed below, Part 3.B.iii.

devices, as the Federal Trade Commission pointed out in its January 2015 staff paper on IoT privacy and security.¹⁷⁶

As to how these issues should be addressed, several commenters felt that the Department of Commerce, for various reasons, is not the place to develop policy in this area. For example, the Consumer Federation of America argued that “[t]he DOC is not the right place to develop U.S. privacy policy. It is not a privacy or consumer protection agency.”¹⁷⁷ And the Niskanen Center stated that “Congress, and not a confusing hodgepodge of competing regulatory bodies, will be the primary regulator of IoT. Congress, not Executive Branch regulators, should lead on the IoT.”¹⁷⁸ There was some support, however, for multistakeholder efforts, both facilitated by the government or in which the government acts as a participant.¹⁷⁹ Multistakeholder efforts call for bringing all interested stakeholders together to try to reach consensus on how to address a particular problem or issue.

One clear argument made by several of the commenters and participants in the workshop is that any approach to privacy policy from the government should be technology neutral. Hewlett Packard argued that the “overall privacy and data protection environment should be flexible enough for new technologies, and not create IoT-specific requirements.”¹⁸⁰ Former Federal Trade Commission Commissioner Julie Brill called for technology-neutral baseline privacy legislation during the IoT workshop.¹⁸¹ Through baseline privacy legislation, such as the Commerce Department’s 2015 Discussion Draft based on the Consumer Privacy Bill of Rights,¹⁸² it would be possible to address privacy concerns without regard to the type of technology used. It would also supplant the current patchwork of regulation based on information type and use.¹⁸³

iii. Intellectual Property

IoT technologies and uses can involve significant intellectual property issues – including copyright, patents, trade secrets, and trademarks – some of which commenters discussed and are highlighted in this section. The comments indicate that, in general, intellectual property is an important topic that deserves recognition and further consideration as IoT penetrates more

¹⁷⁶ Federal Trade Commission, *Internet of Things: Privacy & Security in a Connected World* (January 2015), 14, <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>.

¹⁷⁷ Consumer Federation of America Comment at 7.

¹⁷⁸ Niskanen Center Comment at 7.

¹⁷⁹ See, e.g., Internet Commerce Coalition Comment at 3; Southern Company Services Comment at 3.

¹⁸⁰ Hewlett Packard Enterprise Comment at 2.

¹⁸¹ Fostering the Advancement of the Internet of Things Workshop, September 1, 2016, Transcript at <https://www.ntia.doc.gov/files/ntia/publications/09012016-iot-workshop.pdf>,

¹⁸² Consumer Privacy Bill of Rights Administration Discussion Draft (2015), <https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf>.

¹⁸³ Using a risk-based systems engineering approach to privacy could further facilitate addressing privacy concerns. See NIST research on privacy engineering at http://csrc.nist.gov/projects/privacy_engineering/index.html.

households and businesses and becomes a ubiquitous part of everyday life. Furthermore, as the comments suggest, IoT plays into ongoing intellectual property policy discussions, which address more general concerns.¹⁸⁴ These issues also have international policy implications.¹⁸⁵

1. Copyright

Copyright law protects original works of authorship fixed in a tangible medium of expression by granting to authors certain exclusive rights subject to a number of exceptions and limitations.¹⁸⁶ The United States and many other countries also provide protection against the circumvention of technological protection measures (TPMs) designed to prevent the unauthorized use of or access to works protected by copyright.¹⁸⁷ Key copyright-related IoT issues involve ownership, access, and usage of data and software.

Commenters noted that there are still questions about who owns data in the IoT environment, and what may be done with it.¹⁸⁸ The answers will depend in part on the nature of the “data,” whether it is embodied in a copyrightable compilation, and whether an exception or limitation applies.¹⁸⁹ Although mere “facts” (e.g., the temperature of a home) are not eligible for copyright protection, if data outputs produced by IoT devices include copyrightable sounds or images,¹⁹⁰ or reflect a

¹⁸⁴ For example, some commenters argue that patent assertion entities could stifle development of IoT. *See, e.g.*, Internet Association Comment at 9-11; Nokia Comments at 4; Public Knowledge Comments at 7; Computer & Communications Industry Association Comment at 9. The effect that litigation threats by patent assertion entities have on innovation has been a significant subject of discussion within government and the private sector for a number of years. *See, e.g.*, House Energy and Commerce Committee Hearing on The Impact of Patent Assertion Entities on Innovation and the Economy, <https://energycommerce.house.gov/hearings-and-votes/hearings/impact-patent-assertion-entities-innovation-and-economy>.

¹⁸⁵ For example, TPMs and RMIs, discussed below, are part of bilateral and multilateral copyright treaties. *See* Internet Policy Task Force, *Copyright, Creativity, and Innovation in the Digital Economy*, 16-19 (2013) (“Copyright Green Paper”), <http://www.uspto.gov/sites/default/files/news/publications/copyrightgreenpaper.pdf>.

¹⁸⁶ 17 U.S.C. § 106 (listing exclusive rights of copyright holders).

¹⁸⁷ Section 1201 prohibits the circumvention of TPMs that effectively control access to copyrighted works (“access controls”) and also prohibits trafficking in technologies or services that facilitate circumvention of TPMs that protect copyright owners’ exclusive rights (“copy controls”), 17 U.S.C. § 1201(a)-(b). Section 1201 also includes certain statutory exemptions from the prohibition against circumvention, including for reverse engineering of computer programs to achieve interoperability. *See also* Copyright Green Paper, 16-18, 26-27 (describing TPMs). In addition, every three years the Librarian of Congress may issue temporary exemptions from the prohibition against circumventing TPMs. The Register of Copyrights is required to consult with the Assistant Secretary for Communications and Information at NTIA when considering what exemptions to recommend to the Librarian of Congress in a triennial rulemaking process. 17 USC Section § 1201. Exemptions granted by the Librarian under this rulemaking process last three years but may be renewed in a future proceeding. In addition to TPMs, another technological adjunct to copyright can help protect data integrity and metadata by prohibiting falsifying or removing rights management information (RMI). 17 U.S.C § 1202. *See also* Copyright Green Paper at 19 (describing RMIs).

¹⁸⁸ ACM U.S. Public Policy Council Comment at 4-5 (emphasizing the importance of data ownership, maintenance of data and metadata, and attribution). *See also* Consumer Federation Comment at 4; InterDigital Comment at 6 (urging Commerce department to “look ahead” to data ownership issues); Online Trust Alliance Comment at 5-6; Huawei Technologies Comment at 13.

¹⁸⁹ Software and data may also be subject to trade secret protection, as discussed below.

¹⁹⁰ Dr. Rosner Comment at 3 (noting that IoT includes low-cost webcams); SIA Comment at 1-2, noting that IoT includes video surveillance technologies. CTIA Comment at 4 (“Samsung’s Family Hub refrigerator connects to the

sufficiently original selection and presentation of data,¹⁹¹ then permission may be required to copy, distribute, or modify the resulting works.

Some commenters focused on how licensing terms affect the way in which consumers interact with the copyrighted software embedded in IoT devices, and argued for solutions that would enable consumers to own the copies of software embedded in the devices they purchase.¹⁹² Other commenters stated that it is important that IoT policies do not inadvertently undermine intellectual property rights, or weaken established licensing practices.¹⁹³ One commenter pointed out copyright's important role in deterring counterfeit mobile applications by discouraging counterfeit applications that may carry malware.¹⁹⁴

Some commenters focused on the impact that anti-circumvention provisions may have on access to software and data.¹⁹⁵ Commenters were divided on how these provisions would ultimately affect the development of IoT, and what actions the government should take as a result. For example, one commenter argued that the unrestricted ability to access and modify embedded software will threaten the reliability, safety, and usability of IoT devices.¹⁹⁶ Another wrote that technological protection measures inhibit security research, which they claimed further threatens consumer privacy and security.¹⁹⁷

Internet and mobile devices so that users can order groceries, stream music, and view the contents of their fridge from anywhere"). See also Justin Hughes, *The Photographer's Copyright: Photograph as Art, Photograph as Database*, 25 HARV. J. LAW & TEC. 327 at 367-368, 380-81, 409 (2012) (discussing copyrightability of images produced by surveillance cameras and satellite systems).

¹⁹¹ See U.S. Copyright Office, Cir. 14, *Copyright in Derivative Works and Compilations* (2013) ("copyright in a compilation of data extends only to the selection, coordination or arrangement of the materials or data, but not to the data itself"), <http://copyright.gov/circs/circ14.pdf>.

¹⁹² Consumer Federation of America Comment at 4, 10; Consumers Union Comment at 5; Owners' Rights Initiative Comment. This issue has drawn the attention of Congress, which in October 2015 directed the Copyright Office to review the role of copyright law with respect to software-enabled consumer products. See <http://www.copyright.gov/policy/software/>. The Copyright Office issued its report December 15, 2016, and observed that:

[T]he reach and scope of licensing practices for embedded software [is] an issue that implicates several subsidiary issues, including: the relationship of the Copyright Act to state contract law; whether, and in what circumstances, violations of the terms of software licenses would constitute copyright infringement; and confusion among consumers regarding licensing terms for embedded software. The Office's study found that, in certain circumstances, such as resale, there is only limited evidence regarding real-world restrictions. Accordingly, the Office believes that the question of ownership versus licensing, while very important, is one that can be resolved with the proper application of existing case law.

U.S. Copyright Office, *Software-Enabled Consumer Products: A Report of the Register of Copyrights* at iii (2016), available at <https://www.copyright.gov/policy/software/software-full-report.pdf>.

¹⁹³ BSA | The Software Alliance Comment at 6-7; ACT | The App Association Comment at 10.

¹⁹⁴ ACT | The App Association Comment at 10-11.

¹⁹⁵ See U.S. Chamber of Commerce Center for Advanced Technology and Innovation Comment at 14; Consumer Federation of America Comment at 10; Owner's Rights Comment at 2.

¹⁹⁶ The Software & Information Industry Association Comment at 2.

¹⁹⁷ Electronic Frontier Foundation Comment at 6-9.

2. Patents

As with any technological field, patents can be expected to play a key role in IoT development. By securing exclusive property rights for the inventors of technical advances, patents provide incentives for innovators to develop better IoT devices, manufacturing practices, and infrastructure. Several patent policy issues have the potential to impact IoT industries going forward. At present, none of these issues are unique to IoT,¹⁹⁸ and the USPTO and other federal agencies have been working to address a number of them.

As standards for IoT are developed in the United States and abroad, issues around standard essential patents and licensing may arise,¹⁹⁹ reflecting discussions currently underway in broader sectors such as information and communication technology. When private-sector standards developing organizations (SDOs) develop new consensus standards, some SDOs encourage or require participants to declare any patents they own (or pending patent applications) that would be needed to implement the standard.²⁰⁰ For its part, the U.S. Government, based on longstanding policy,²⁰¹ defers to private sector SDOs to adopt approaches that meet the needs of the participating members and the industries where those standards will be used while appropriately balancing the various interests involved while fairly compensating patent owners for use of their technology.²⁰²

¹⁹⁸ Indeed, one commenter noted the importance of accounting for the impact of these issues on the broader economy rather than just the narrow confines of IoT. *See* Fashion Innovation Alliance Comment at 4.

¹⁹⁹ *See* Ericsson Comment at 2, 14; Staff of the Federal Trade Commission's Bureau of Consumer Protection and Office of Policy Planning Comment at 15; ACT | The App Association Comment at 6.

²⁰⁰ *See* Fed. Trade Comm'n, Prepared Statement of the Fed. Trade Comm'n before the United States Senate Comm. on the Judiciary Subcommittee on Antitrust, Competition Policy and Consumer Rights concerning Standard Essential Patent Disputes and Antitrust Law at 4-6 (July 30, 2013),

https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commissionconcerning-standard-essential-patent-disputes-and/130730standardessentialpatents.pdf (cited by Staff of the Federal Trade Commission's Bureau of Consumer Protection and Office of Policy Planning Comment at 1, 84; ACT | The App Association Comment at 6. Most SDOs require participants to affirm whether they are willing to license any patents that are required to implement the standard, and if so, whether they are willing to license them on terms that are reasonable and non-discriminatory. Such standard essential patents are then subject to the SDO's patent licensing policy, which may require licensing the patents on fair, reasonable, and non-discriminatory (FRAND) terms to anyone using the standard.²⁰⁰ In addition, several commenters suggested that governments should assist in addressing or resolving these standards-related policy differences. ACT | The App Association Comment at 6-10; Cisco Systems Comment at 15-17, 30; Ericsson Comment at 2, 14; Internet Association Comment at 9-11; Nokia Comment at 3-4, 11; Qualcomm Comment at 14-15; Microsoft Comment at 12.

²⁰¹ *See* OMB Circular A-119, https://www.whitehouse.gov/omb/circulars_a119; University of Michigan Comment at 1.

²⁰² In some situations, however, certain U.S. Government policymakers may have weighed in with non-binding policy statements, such as with the 2013 policy statement from the USPTO and the Department of Justice on litigation remedies for standard essential patents under FRAND commitments.

https://www.uspto.gov/about/offices/ogc/Final_DOJ-PTO_Policy_Statement_on_FRAND_SEPs_1-8-13.pdf.

Patent quality is another critical issue that attracted considerable attention among stakeholders, particularly with regard to litigation.²⁰³ The Department recognizes that clarity is important for letting industry competitors and the public know which functionality or actions are covered by a patent, when they should seek licenses, and what alternatives they can pursue. USPTO has been actively engaged on this topic with the patent community.²⁰⁴ Commenters also stated that the government should address patent trolls and reduce abusive patent litigation, according to two commenters.²⁰⁵

One commenter noted the importance of providing clear eligibility for patentable subject matter in the IoT space.²⁰⁶ In response to several Supreme Court cases that altered longstanding practice on eligibility, the USPTO issued guidance to patent examiners in 2014 on how to apply the Supreme Court's rulings during examination, and has been providing regular updates and teaching examples with substantial input from patent stakeholders as new court cases are decided.²⁰⁷

The Niskanen Center stated that IoT may likewise present challenges for enforceability of patents.²⁰⁸ For instance, the distributed nature of IoT may raise a number of questions regarding multi-party infringement liability. Traditionally, one party must perform every element of a patent claim to be liable for infringement. However, sometimes multiple parties act together in such a way that the combined result performs the patent claims. Patent owners have limited mechanisms to enforce their patents in such situations.²⁰⁹ However, these types of liability have

²⁰³ Computer & Communications Industry Association Comment at 9-10; Consumer Technology Association Comment at 8; Internet Association Comment at 9-11; Public Knowledge Comment at 7-8.

²⁰⁴ Recognizing the need for high-level, systemic, and operational focus on this issue, the USPTO appointed its first Deputy Commissioner for Patent Quality in 2015 and launched its “Enhanced Patent Quality Initiative” (EPQI) soon after. These efforts help to improve the clarity of the patent record (including patent scope) and increase certainty that the patent was granted in accordance with applicable statutory requirements. *See* USPTO Enhanced Patent Quality Initiative, <http://www.uspto.gov/patent/initiatives/enhanced-patent-quality-initiative-0>. *See also*, [Comment of the United States Federal Trade Commission and the United States Department of Justice Before the United States Department of Commerce Patent and Trademark Office: In the Matter of Request for Comments on Enhancing Patent Quality](https://www.ftc.gov/policy/policy-actions/advocacy-filings/2015/05/comment-united-states-federal-trade-commission-united), <https://www.ftc.gov/policy/policy-actions/advocacy-filings/2015/05/comment-united-states-federal-trade-commission-united>.

²⁰⁵ *See* Public Knowledge Comment at 7; Annex to Nokia Comment at 2; Computer & Communications Industry Association Comment at 8. *See also*, Patent Assertion Entity Activity: An FTC Study, <https://www.ftc.gov/reports/patent-assertion-entity-activity-ftc-study>.

²⁰⁶ Niskanen Center Comment at 23.

²⁰⁷ *See* USPTO 2014 Interim Guidance on Subject Matter Eligibility, <http://www.uspto.gov/patent/laws-and-regulations/examination-policy/2014-interim-guidance-subject-matter-eligibility-0>.

²⁰⁸ *See, e.g.*, Niskanen Center Comment at 20, 22.

²⁰⁹ Namely: divided infringement, where one actor directs or controls the actions of another, or when multiple actors engage in a “joint enterprise” to perform all the steps of a patent claim (*See Akamai Techs., Inc. v. Limelight Networks, Inc.*, 797 F.3d 1020 (2015)); active inducement, where one party induces another party to perform steps which infringe a patent claim (35 U.S.C § 271(b)). *See Commil USA, LLC v. Cisco Sys.*, 135 S. Ct. 1920 (2015); and contributory infringement, where one actor sells a material part of a patented invention for use by others to infringe the patent (35 U.S.C. § 271(c)).

limitations that can make it difficult to enforce certain patents, particularly since the Internet allows seamless, invisible, efficient interactions by multiple parties.

3. Trade Secrets

A trade secret is confidential, commercially valuable information that provides a company with a competitive advantage, such as customer lists, methods of production, marketing strategies, pricing information, and chemical formulae.²¹⁰ The type of information that could be protected as a trade secret is virtually limitless. At issue is how trade secret protection promotes IoT innovation, and how the rise of IoT impacts trade secret protection.

Trade secrets are crucial to helping our entrepreneurs and businesses start, grow, and innovate, including in the IoT space. In addition, the proliferation of devices and connectivity that makes up IoT also gives rise to trade secret vulnerabilities.²¹¹ In relation to IoT, one commenter posited that “[p]roducts will be defined by the sophistication of their algorithms. Organizations will be valued based not just on their big data, but the algorithms that turn that data into actions and ultimately customer impact.”²¹² The protection and security of algorithms associated with IoT has been noted as an issue.²¹³ Accordingly, the protection of trade secrets is one key element to the encouragement of innovation in the IoT sphere.

Confidentiality concerns were mentioned by some commenters.²¹⁴ In business environments, data sharing without appropriate controls to protect against inadvertent release of confidential information creates additional risk that trade secrets will be exposed. Only one commenter specifically mentioned the implication of these general concerns for trade secrets, although other

²¹⁰ Yeh, Brian, *Protection of Trade Secrets: Overview of Current Law and Legislation*, Congressional Research Service Report No. R43714 (April 2016). <http://www.fas.org/sgp/crs/secretary/R43714.pdf>.

²¹¹ One requirement of trade secret protection is that the information must be subject to reasonable efforts to maintain secrecy. “Technologies providing greater access to information anytime and anywhere will increasingly rely on the internet, and present new challenges to companies seeking to protect information transmitted by, or contained on, mobile devices.” White House, Strategy on Mitigating the Theft of US Trade Secrets (2013), https://www.whitehouse.gov/sites/default/files/omb/IPEC/admin_strategy_on_mitigating_the_theft_of_u.s._trade_secrets.pdf. The same report notes that the cultural, economic, and geopolitical shifts, in particular as employees can work and access data anywhere and at any time, not just at an office, laboratory, or factory, creates additional risks to trade secrets.

²¹² Peter Sondergaard, The Internet of Things Will Give Rise to the Algorithm Economy (June 1, 2015), available at: <http://blogs.gartner.com/peter-sondergaard/the-internet-of-things-will-give-rise-to-the-algorithm-economy/>

²¹³ David Levine, What Does the Internet of Things Mean for Corporate Secrecy? Slate, (April 4, 2014), available at: http://www.slate.com/blogs/future_tense/2014/04/04/what_does_the_internet_of_things_mean_for_corporate_secrecy.html.

²¹⁴ James Andrew Lewis, *Managing Risk for the Internet of Things*, Center for Strategic and International Studies (Dec. 2015), https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151201_Lewis_ManagingRiskIoT_Web.pdf. “IoT does not change the most important problem we currently face in data and network protection – data exfiltration leading to the theft of intellectual property, business confidential information, and personal information. Most IoT devices will not store intellectual property or business confidential data.”

references to proprietary, confidential, and/or sensitive information could be considered to relate to trade secrets as well.²¹⁵

4. Trademark

According to some commenters, the creation of platforms for interoperability of products and services creates opportunities for trademark owners to diversify their brand offerings but raises enforcement challenges.²¹⁶ Trademarks serve several functions for consumers and brand owners, including serving as quality indicators as well as signaling who is responsible for a substandard product.²¹⁷ Some commenters said that products falsely alleged to be compatible with a suite of proprietary branded devices or services could engender performance deficits that affect the operation of the branded products and subject the brand owner to lawsuits.²¹⁸ Use of the brand by third parties to signal interoperability presents enforcement costs as well as licensing opportunities.²¹⁹ Notably, there may be a significant role for use of certification trademarks to indicate that goods have been certified as meeting standards for device interoperability.²²⁰ These challenges are not specific to IoT, but should be considered when deciding how best to leverage brands using these new technologies.

iv. Free Flow of Data Across Borders

The free and open global Internet, with minimal barriers to the flow of information and services across national borders, is the lynchpin of the digital economy today.

²¹⁵ Niskanen Center Comment at 27 (noting that encryption can protect trade secrets).

²¹⁶ *See, e.g.*, AT&T Services Comment at 11-12 (discussing branding strategies in the context of different business models); Fashion Innovation Alliance Comment at 4 (discussing fashion brands that could be looking to integrate technology into their apparel and accessories); Annex to Comments of Internet Society at 47 (“some device manufacturers see a market advantage to creating a proprietary ecosystem of compatible IoT products... which limit interoperability to only those devices and components within the brand product line”); Comments of Security Industry Association at 3.

²¹⁷ *See, e.g.* Riley Walters Comment at 3 (observing that device security is beneficial to the IoT producer brand name).

²¹⁸ ACT | The App Association Comment at 10 (misappropriating application logic and brands to create counterfeit software applications that harm the IoT environment). Center for Strategic and International Studies Comment at 4 (manufacturer brand owners must do a risk assessment for lawsuits and liability costs if a car is shown to be unsafe because it is vulnerable to hacking).

²¹⁹ U.S. law requires trademark owners to control the quality of the goods or services bearing their brand, even when the brand is licensed for use by authorized third parties.

²²⁰ Certification trademarks may be used to certify that authorized users’ goods or services meet certain standards in relation to quality, materials, or mode of manufacture (e.g., approval by Underwriters Laboratories). 15 U.S.C. §§ 1054, 1127. *See* Open Connectivity Foundation Comment at 2 (noting that it provides branding for certified IoT devices via compliance testing).

A number of commenters emphasized just how important a free and open Internet is to the future innovation and growth of IoT.²²¹ They stressed that cross-border information flows are critical to companies across sectors, from industrial to human resources. While some governments have created policies that limit cross-border data flows for various reasons, such policies could negatively affect the growth of certain IoT sectors by impeding the normal functioning of the devices, many of which themselves cross borders frequently (e.g., sensors on an airplane). Further, these commenters argued that these policies raise costs, especially for small and medium sized companies, which can slow economic growth.

Multiple commenters recommended that the U.S. Government continue to work with the international community to encourage the cross-border flow of data to enable IoT services and discourage forms of localization.²²² This might include work on interoperability of privacy and cybersecurity regimes and standards. Stakeholders also recommended that the U.S. Government should seek to form binding commitments with other nations to ensure the flow of information.²²³

v. Planned Activities

The Department reaffirms its commitment to the policy approach that has made the United States the leading innovation economy. This approach is reflected in the 1997 Framework for Global Electronic Commerce,²²⁴ and has been maintained across all subsequent Presidential administrations. It asserts that policy should generally be industry led, and that regulation, when needed, should be predictable and consistent. The Department is positioned to advance U.S. policy approaches around IoT, including those recommended in this paper. Policy related to IoT spans multiple domains from data protection and privacy issues, to infrastructure stability and security, to digital inclusion. The following issues are and will continue to be priority focus areas of the Department in the IoT domain.

1. *Current Initiatives*

- **International Engagements.** Government-to-government dialogues and relevant international fora are major vehicles for the Department's international engagement on IoT. Currently the Department maintains formal dialogues with numerous governments where digital economy and general information and communications technology issues are often discussed. Through stakeholder input, the Department envisions IoT and aspects

²²¹ See, e.g., Visa comment at 7; Computer & Communications Industry Comment at 6; Trans-Atlantic Business Council Comment at 9; Information Technology Industry Council Comment at 5, Security Industry Association Comment at 4.

²²² Visa Comment at 7; Nest Labs Comment at 14-15; ACT | The APP Association Comment at 11-12.

²²³ See, e.g., Nest Labs Comment at 14-15; BSA | The Software Alliance Comment at 6; Computer & Communications Industry Association Comment at 6; IBM Comment at 3.

²²⁴ The White House, The Framework for Global Electronic Commerce, (July, 1997)

<http://clinton4.nara.gov/WH/New/Commerce/>.

thereof will continue to be raised in these engagements. In international fora, the Department engages in the work of the International Telecommunication Union and in the Internet Governance Forum (IGF) IoT dynamic coalition, among others.

- **Interagency Collaboration.** The Department will continue to work with its interagency partners to ensure the development of policy that fosters IoT innovation and protects the rights and safety of individuals.
- **Cybersecurity.** The Department will continue to bring private sector experts together with policymakers to define security principles for IoT, facilitate IoT security framework development by sector and application, and encourage the implementation of best practices and/or minimum standards.
 - **NTIA Cybersecurity Multistakeholder Process.** NTIA is convening a cybersecurity-focused multistakeholder process to address IoT security upgradability and patching.²²⁵ The objective of this multistakeholder process is to foster a market offering more devices and systems that support security upgrades through increased consumer awareness and understanding. Enabling a thriving market for patchable IoT devices requires common definitions so that manufacturers and solution providers speak a common language.

As the process identified, IoT has brought connectivity to business sectors that previously did not provide networked products – and some of these businesses are confronting a new requirement to deal effectively with cybersecurity threats targeting their products. The Department is assisting by working with industry and other stakeholders to document best practices for patching, vulnerability notification, and control of data retention for IoT products. In addition, the threat posed by orphan devices – devices no longer supported by their manufacturers – must also be addressed. Devices that consumers continue to use to connect to the Internet should be updated and protected even if device manufacturers discontinue them. There should be some mechanism (such as transferring the needed software keys to a designated consortium) for ensuring that devices function with the software updates needed to ensure security. Stakeholders, through NTIA’s multistakeholder process, will have the opportunity to encourage providers of connected devices and services to embrace security-by-design, beginning with risk assessment as part of the design process, testing security measures before products and services launch, and using encryption to store and use sensitive information.

²²⁵ <https://www.ntia.doc.gov/files/ntia/publications/2016-22459.pdf>

- **Privacy.** The Department continues to address privacy concerns in a range of contexts, from support for baseline privacy legislation that would include IoT services, to work to promote the availability of strong encryption (including in IoT devices).
- **Intellectual Property.** The Department of Commerce will continue to work to promote the positive evolution of intellectual property and its protection in the Internet’s digital economy. Over the past few years, the Department has consulted extensively with stakeholders. It produced a green paper on *Copyright Policy, Creativity, Innovation, and the Digital Economy*,²²⁶ which provided a thorough and comprehensive analysis of digital copyright policy, including issues relevant to the Internet of Things. It published a White Paper on *Remixes, First Sale, and Statutory Damages*,²²⁷ and is conducting work as recommended in those papers, including facilitating discussions about standards and interoperability in the context of developing the online marketplace for copyrighted works.
- **Cross-Border Data Flows.** Recognizing the value of Internet openness and the free flow of information, and the risks that restrictions on Internet data flows present to innovation, economic growth, and social prosperity, the Department of Commerce has made it a top priority to ensure that information and data continue to flow freely and the Internet remains open and global. The Department has played a critical role in developing policies and initiatives that protect the free flow of information and foster a robust digital economy. For example, the Department championed the development of the *Principles for Internet Policy-Making* at the Organization for Economic Cooperation and Development (OECD).²²⁸

2. Proposed Next Steps

The Department will:

- Continue to foster an enabling environment for IoT technology to grow and thrive, allow the private sector to lead, and promote technology-neutral standards and consensus-based multistakeholder approaches to policy making at local, tribal, state, federal, and international levels on issues ranging from U.S. security and competitiveness to

²²⁶ <https://www.uspto.gov/learning-and-resources/ip-policy/copyright/green-paper-copyright-policy-creativity-and-innovation>

²²⁷ <https://www.uspto.gov/learning-and-resources/ip-policy/copyright/white-paper-remixes-first-sale-and-statutory-damages>

²²⁸ Organization for Economic Cooperation and Development (OECD), *Principles for Internet Policy-Making* (2014), <http://www.oecd.org/sti/ieconomy/oecd-principles-for-internet-policy-making.pdf>.

cybersecurity, privacy, intellectual property, the free flow of information, digital inclusion, interoperability, and stability related to IoT.

- Identify and, where appropriate, convene multistakeholder processes on IoT policy issues based on stakeholder feedback in areas such as cybersecurity, privacy, inclusion, intellectual property, and cross-border data flows.
- Proactively engage and collaborate with other relevant agencies on IoT in order to protect the safety and rights of individuals, promote innovation, and ensure a consistent and predictable regulatory environment, such as with the Department of Homeland Security,²²⁹ the Department of Transportation,²³⁰ and the Food and Drug Administration,²³¹ among others.
- Leverage its country and industry experts and work closely with key interagency partners toward a consistent and predictable international IoT policy environment based on bottom-up, industry-led solutions.
- **Cybersecurity.**
 - Proactively support and promote cybersecurity policy for the IoT environment that encourages risk-based approaches, security by design, and the ability to fix or “patch” insecure software and devices.
 - As one of the key tools for addressing IoT cybersecurity concerns, promote the use of strong encryption in IoT services and products to address security concerns in the government’s risk-based approach to the use and application of IoT technologies.
 - Collaborate with industry to educate consumers on issues such as how to limit risks associated with unsecured connected devices (e.g., by changing default passwords, using password-protected home Wi-Fi networks, and employing virtual private networks).
 - On December 2nd, 2016, the Presidential Commission on Enhancing National Cybersecurity presented its report to the President, which included several recommendations specific to IoT. The Department welcomes the Commission’s

²²⁹ See <https://www.dhs.gov/securingtheIoT>

²³⁰ See <https://www.transportation.gov/AV>

²³¹ See <http://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm>

endorsement of the Department's leadership role in helping to guide cybersecurity policy, and is carefully reviewing and considering the Commission's recommendations as we move forward in our efforts to meet the nation's cybersecurity needs.

- **Privacy.** Work to address the need to protect consumer privacy in the IoT environment, and continue to support baseline privacy legislation, as well as an engineering approach to privacy.
- **Intellectual Property.** Work to promote the positive evolution of intellectual property and its protection in the digital economy.
- **Cross-Border Data Flows.** Work with its international partners toward an industry-led global marketplace that promotes innovation for IoT and supports the free flow of information, and the ability of American companies to compete fairly around the world.

C. Promoting Standards and Technology Advancement

Numerous commenters called attention to the important role of the U.S. Government in the context of supporting the development of IoT standards, and many agreed that the U.S. Government should encourage industry-led efforts toward the adoption of voluntary, consensus-based, global standards for IoT.²³² Commenters also noted that interoperability and related standards development will be important to the success of IoT from a technical perspective, and the U.S. Government should actively support these national and international industry-led efforts.²³³ A wide range of standards addressing different aspects of IoT applications – technology, connectivity, interoperability, functionality, security, usability, etc. – will be needed.

i. Standards Development

It is the Department's position that a private-sector-led approach to standards development with appropriate government participation is fundamental to successfully developing these standards. While GS1 was concerned about the confusion that could arise from too many standards,²³⁴ Infineon and CA Technologies discussed the way in which a diversity of industry-led standards organizations will be able to address the various aspects of the IoT environment and will likely converge.²³⁵ Underscoring the need for a diverse set of industry-led, globally relevant IoT standards activities, the American National Standards Institute referenced the World Trade

²³² Software & Information Industry Association Comment at 12; Symantec Comment at 4-5; Visa Comment at 7; Cisco Systems Comment at 30; Consumer Technology Association Comment at 8-9.

²³³ See AIM Comment at 8; AIM North America Comment at 8; Alliance of Automobile Manufacturers at 6; Local Innovation Comment at 7; National Association of Realtors Comment at 2.

²³⁴ See; GS1 US Comment at 14-15.

²³⁵ See CA Technologies Comment at 2; Infineon Technologies Americans Comment at 5.

Organization Technical Barriers to Trade Agreement Committee Decision, which states that the global relevance of a standard is determined by how it was developed, not by where it was developed.²³⁶ Given the systems engineering nature of IoT applications, it is not surprising that different standards and specifications address different needs in each layer of the system stack. A range of standards organizations are already enabling standards development that is private-sector led, open, voluntary, consensus-based, and nimble.²³⁷ New organizations are being established to meet IoT standards and specification needs as applications evolve for IoT technology.

Industry, with active participation from government experts as needed, is ideally positioned to lead the development of technological standards and solutions to address global IoT environment opportunities and challenges. The American National Standards Institute strongly advocated for the multiple-path approach to IoT standardization. Under the multiple-path approach, the relevance and utility of a standard is not linked to the organization that developed it, and multiple or competing standards can be used as solutions to meet given requirements. It added that this will help sustain a level playing field for standards organizations in which standards have been developed in a balanced, open, consensus-based process.²³⁸ The Consumer Technology Association suggested that an emphasis on commercial solutions and market-developed voluntary standards would foster faster adoption of IoT and increased innovation.²³⁹

Commenters pointed to the fact that governments can work as both facilitator and convener to identify standards needs and priorities, and in such instances, they should ensure full industry participation in these processes.²⁴⁰ The Information Technology Industry Council urged the Department to strongly encourage governments to participate in industry-led standardization activities, but governments should not take the lead or direct development of standards.²⁴¹ In

²³⁶ American National Standards Institute Comment at 2; National Association of Manufacturers Comment at 2.

²³⁷ See <http://www.consortiuminfo.org/links/linksall.php> for a full list of information and communication technology standards organizations.

²³⁸ American National Standards Institute Comment at 2.

²³⁹ Consumer Technology Association Comment at 9 (citations omitted).

²⁴⁰ See Software & Information Industry Association Comment at 6; L Jean Camp, Ryan Henry, Steven Meyers, Gianpaolo Russo Comment at 5; AT&T Services Comment at 35-36. The Department follows guidance laid out in the Memorandum on Principles for Federal Engagement in Standards Activities to Address National Priorities (M-12-08), jointly issued by the Executive Office of the President's Office of Management and Budget, Office of the U.S. Trade Representative, and Office of Science and Technology Policy.

<https://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-08.pdf>.

²⁴¹ See, for a fuller description of the current USG approach to standards development, https://www.whitehouse.gov/omb/inforeg_infopoltech; <https://www.whitehouse.gov/blog/2014/02/14/updating-guidance-use-voluntary-consensus-standards-promote-smarter-regulation-col-0>; This approach is set out in OMB Circular A-119, Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities (revised January, 2016). See also, OMB Memorandum M-12-08 (January, 2016), https://www.whitehouse.gov/sites/default/files/omb/memoranda/2012/m-12-08_1.pdf, which states: "The vibrancy and effectiveness of the U.S. standards system in enabling innovation depend on continued private-sector leadership and engagement. Most standards developed and used in U.S. markets are created with little or no government involvement. This approach – reliance on private sector leadership, supplemented by federal government

cases where multilateral organizations wish to lead standards efforts, the Information Technology Industry Council suggested those organizations should allow full industry participation, and should avoid engaging in standardization activities that may duplicate, or even conflict with, global industry-led IoT standards.²⁴²

Due to the vast and expansive nature of the technologies underpinning IoT, no single standards developing organization has the resources or the expertise to develop all of the standards that will be needed. Commenters have called attention to the important role the U.S. Government could play in advocating for the development and use of international standards and specifications developed in industry-led efforts that are voluntary, consensus-based, and open to participation by interested stakeholders.²⁴³

Commenters specifically detailed the U.S. Government's ongoing role in United Nations agencies such as the International Telecommunication Union's Standardization Sector (ITU-T) and the World Intellectual Property Organization, where IoT activities are currently underway.²⁴⁴ Various commenters noted concerns about the ITU-T.²⁴⁵ Comments covered concerns with proposed scope and the potential for duplication of work underway in other standards organizations.²⁴⁶ Commenters urged the U.S. Government to encourage international partners to support the development and use of international standards to the extent practicable and advocate against standards that are developed in processes that are not open to all interested stakeholders or that do not treat all stakeholders in a similar manner.²⁴⁷ Concern was also expressed about standards development activities that do not have strong industry support or participation.²⁴⁸ To prevent possible market access barriers, commenters generally agree that the U.S. Government

contributions to discrete standardization processes ... – remains the primary strategy for government engagement in standards development. Consistent with the Administration's commitment to openness, transparency, and multi-stakeholder engagement, all standards activities should involve the private sector."

²⁴²Information Technology Industry Council Comment at 12 (citations omitted).

²⁴³Semiconductor Industry Association Comment at 5; Trans-Atlantic Business Council Comment at 10; Telecommunications Industry Association Comment at 2. This approach is consistent with the longstanding policies of the U.S. Government, which has articulated the importance of the decision contained in Annex 2 of the Decisions and Recommendations adopted by the WTO's TBT. The TBT Committee stated that principles and procedures for transparency, openness, impartiality, consensus, effectiveness and relevance, coherence and addressing the concerns of developing countries should be observed when international standards are being developed (G/TBT/1 Rev 12, 2015). TBT Committee, G/TBT/1/Rev.12 (2015), https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S009-DP.aspx?language=E&CatalogueIdList=129845,121467,101299,87898,63749,11467,12694,21998,31618,23495&CurrentCatalogueIdIndex=0&FullTextHash.

²⁴⁴GSM Association Comment at 20; Niskanen Center Comment at 20-21, 34; Ericsson Comment at 11.

²⁴⁵See Internet Society Comment at 16; 5G Americas Comment at 9; U.S. Chamber of Commerce Center for Advanced Technology and Innovation Comment at 18.

²⁴⁶Verizon Comment at 17, 24; U.S. Chamber of Commerce Center for Advanced Technology and Innovation Comment at 18.

²⁴⁷AIM Comment at 3; U.S. Council for International Business Comment at 2-3.

²⁴⁸5G Americas Comment at 9. GSM Association Comment at 20.

should continue to press adoption of standards that are developed in an open, globally relevant manner.²⁴⁹

Market forces will undoubtedly shape IoT development and innovation. The Department of Commerce agrees with commenters that an industry-led, bottom-up, consensus-based approach to standards development is necessary to realize the benefits of the technology.

ii. Planned Activities

The U.S. Government fosters an industry driven, private sector-led consensus-based approach to standards development. In some other countries or regions, however, governments can have a distorting effect by identifying and directing standardization priorities and funding the development of those priorities to favor their own entities, or where participation and/or decision making in standards organizations is not open to all interested stakeholders, approaches developed may not effectively address the needs of IoT. The rationale provided by governments for active and often interventionist roles in standards development is that it is required by national/regional laws or policies, to support government policies and legislation, or to foster the development of standards to meet requirements that are unique to that country or region. It is clear from commenters that technical standards need to be developed and maintained in order to ensure that IoT reaches its full potential. This will require all parties to work within voluntary consensus standards development bodies to ensure the development, deployment, and interoperability of the IoT environment. The Department will continue to support IoT standards development that is bottom up and private-sector led. Technology development in the form of hardware and software advancement and new applications and devices will also be critical to IoT growth and adoption.

1. *Current Initiatives*

- **The Cyber-Physical Systems Public Working Group (CPS PWG)**, formed by NIST in 2014, brings together experts to help define and shape key aspects of cyber-physical systems to accelerate their development and implementation within multiple sectors of our economy. Through its five subgroups, the CPS PWG has prepared a Cyber-Physical Systems Framework.
- **The Global City Teams Challenge** is a NIST initiative to advance the deployment of IoT technologies within a smart city environment. Nearly 100 teams or “action clusters” are pursuing projects related to energy, transportation, public safety, and other key sectors.

²⁴⁹ American National Standards Institute Comment at 2; ARM Comment at 12; BSA | The Software Alliance Comment at 2; Microsoft Comment at 1.

- **The International Technical Working Group on IoT-Enabled Smart Cities Framework** is a NIST effort comparing and distilling current architectural efforts among the many smart city projects currently underway around the world. The goal is to produce a consensus framework document of common architectural features that will help cities employ interoperable and scalable smart city solutions that will meet the needs of their communities.
- **CPS Research and Standards Development** are carried out in multiple NIST laboratories, including programs in advanced manufacturing, cybersecurity, buildings and structures, disaster resilience, and smart grid.
- **NTIA Monitoring of ITU-T Study Group 20.** NTIA will continue to monitor the activities of the Standardization (ITU-T) Study Group 20 on the Internet of Things and Smart Cities and communities (SC&C), which is studying IoT, its applications, and big data aspects of IoT Smart Cities.
- **Cybersecurity for IoT Program** The NIST Cybersecurity for IoT Program focuses on fundamental and applied research and the transfer of these to industry to enable technology advancement and innovation. NIST has active ongoing work in fundamental research, including standards and guidance, that address security (e.g., [lightweight encryption](#); [RFID](#) and [Bluetooth security](#); systems security engineering; industrial control systems security; and blockchain). Applied research for IoT security at NIST focuses on work to address market-focused application of research through partnering with industry verticals such as Health Information Technology, Vehicle/Transportation, Smart Home and Manufacturing. For example, the [National Cybersecurity Center of Excellence \(NCCoE\)](#) engineers are working with the health care community to address [wireless infusion pump security](#) in hospital environments and publish best practices to address commonly found security risks.

2. Proposed Next Steps

The Department will:

- Monitor IoT related technology developments and applications and contribute to research and development involving those technologies.
- Advocate for industry-led, consensus-based, international standards for IoT technologies and applications in its bilateral and multilateral engagements.
- Actively participate in, and contribute to, the development of technical standards for IoT.

D. Encouraging Markets

Beyond the research and development work done by NTIA, NIST, and other government agencies, the U.S. Government as a whole, and the Department of Commerce in particular, can help to encourage the development and growth of the market for IoT devices by being a leading consumer and adopter of IoT; help to address the workforce issues that will arise due to the deployment of IoT; and help to better understand, plan for, and respond to IoT through quantification and measurement.

i. Public-Private Partnerships and Government Procurement

The U.S. Government is relevant not only as a potential policy maker and regulator, but also as an enabler and adopter. The Public sector can be a leading adopter of emerging technologies, helping to promote compatible regulatory regimes on security, privacy, and intellectual property, as well as transparent and predictable market access regimes. As the Center for Data Innovation commented, “the federal government can reduce the perceived risk of the technology that limits investment and adoption by the private sector and state and local governments. The government should actively pursue opportunities to deploy connected technologies to improve mission delivery, as well as comprehensively examine opportunities to transform agency operations around the potential of the Internet of Things and the data it generates.”²⁵⁰

In addition, the Department plays an important role in educating foreign markets about the benefits of new and emerging technologies, and in promoting U.S. technologies in those arenas. The Department also measures market changes, educates policymakers and the public about market developments, and designs and promotes policies that prepare the U.S. economy for changes that emerging technologies may bring.

ii. Workforce Issues: Education, Training, and Civil Liberties

Over the past two decades, the Internet has spurred incredible innovation in the U.S. economy and positioned the United States as a global leader in information technology, according to the Consumer Technology Association.²⁵¹ In particular, advances in IoT are enabling efficiency in the home and workplace, and delivering more narrowly tailored services to businesses and consumers. As Ligado Networks suggested: “US manufacturers will gain a significant competitive advantage by lowering costs and enabling production efficiencies, reinvigorating domestic production, and allowing US manufacturers to compete with low-cost manufacturers globally.”²⁵² BSA | The Software Alliance noted that by 2020, there will be more than 50 billion

²⁵⁰ *Id.* and Cisco Systems Comment at 10.

²⁵¹ *See* Consumer Technology Association Comment at 5.

²⁵² Ligado Networks Comment at 17.

connected devices relied upon by consumers, governments, and businesses,²⁵³ and Ligado said that, by 2025, 80 percent of U.S. manufacturers will have implemented IoT technologies.²⁵⁴

However, the growth potential could stall without adequate preparation for an economy that relies more heavily on IoT. The State of Illinois commented that IoT will allow for U.S. manufacturers and businesses to increase automation and efficiencies, perhaps increasing the pressure to eliminate jobs that may no longer be needed as the technology may be more cost-effective.²⁵⁵ In order for the United States to take full advantage of developments in an IoT economy, the U.S. Chamber of Commerce Center for Advanced Technology and Innovation suggests that the Department will need to prepare U.S. workers for a shift in workforce education and training needs.²⁵⁶ Recommendations from commenters include:

- Education incentives (e.g., grants, scholarships) for key IoT-related professions such as data science and engineering.²⁵⁷
- Partnerships with universities to develop specialized curricula.²⁵⁸
- Training opportunities (e.g., seminars, workshops) for businesses adopting IoT technologies.²⁵⁹

Education and training are not the only challenges of a workforce conversion in light of IoT adoption. The American Bar Association believes the Department will need to pay attention to individual worker rights and liberties, as some uses of IoT could be invasive (e.g., employee monitoring) or discriminatory.²⁶⁰ Scott R. Peppet of the University of Colorado School of Law commented that an employer could use data from an employee's Fitbit device to infer employee behavior.²⁶¹ This is problematic for several reasons, including that the device could be giving the wrong location. The Federal Trade Commission described in their comments how data on employee commuter distance could, depending on how it is used, violate the equal-employment-opportunity standards.²⁶² These examples reveal the chasm between the data analysis potential that serves both as a driver for efficiency and innovation and as a potential harbinger for civil rights abuses if not managed to account for these issues. If these changes are not properly addressed, as the State of Illinois commented, low-skilled laborers who may not receive the

²⁵³ BSA | The Software Alliance Comment at 4.

²⁵⁴ Ligado Networks Comment at 17.

²⁵⁵ See State of Illinois Comment at 22; Motorola Solutions Comment at 4.

²⁵⁶ See U.S. Chamber of Commerce Center for Advanced Technology and Innovation Comment at 17.

²⁵⁷ See Booz Allen Hamilton Comment at 15.

²⁵⁸ See Cisco Systems Comment at 29.

²⁵⁹ See *Id.*

²⁶⁰ See American Bar Association Section of Science and Technology Law Comment at 7.

²⁶¹ See Scott R. Peppet Comment at 29.

²⁶² See Staff of the Federal Trade Commission's Bureau of Consumer Protection and Office of Policy Planning Comment at 9.

training and resources needed to stay relevant could find themselves at a disadvantage compared with other workers.²⁶³

iii. Quantifying the IoT Sector

The Request for Comment asked several questions regarding whether, and how, the government should measure the IoT sector and its economic impact. Most commenters did not address these questions, and those who did suggested that quantification of IoT was not a high priority. Several commenters even advised against government measuring IoT at this stage. The Competitive Carriers Association recommended not “formulating premature quantification and metrics”²⁶⁴ while the GSM Association suggested that the private sector is best-positioned to quantify the benefits of IoT, such as cost savings, productivity growth, and other efficiencies.²⁶⁵ In contrast, the Center for Data Innovation suggested that government should make measuring IoT a priority, citing the importance of understanding the role of IoT in the industrial value chain, as well as which sectors are adopting IoT rapidly and which are not.²⁶⁶ In particular, they recommended focusing on understanding the value generated by IoT devices as components of the industrial value chain and measuring IoT as part of the broader technology spending.²⁶⁷ With respect to analytic techniques, Booz Allen Hamilton suggested that “IoT lends itself to traditional measures and forecasts of economic impact,” combining broad estimates of economic activity tied to IoT and more targeted impact assessment. Given the complexities of IoT, however, Booz Allen noted that the targeted impact assessment approach would require careful differentiation of which components should be considered IoT and which should not.²⁶⁸ Additionally, the commenter also suggests that “IoT may necessitate development of new cross-industry or cross-system measures,” in which case the government should leverage its “cross-industry working groups or stakeholder listening discussions to gather information” about what and how to measure.²⁶⁹ The Department will take these comments into consideration in its future information-gathering efforts regarding IoT.

iv. Planned Activities

It is clear from commenters that the government can play an important role in fostering the development of IoT through government application, procurement, and international engagements.²⁷⁰ The Department is already actively engaged in promoting innovation both

²⁶³ See State of Illinois Comment at 22.

²⁶⁴ See Competitive Carriers Association Comment at 24.

²⁶⁵ See GSM Association Comments at 14.

²⁶⁶ See Center for Data Innovation Comment 16-17.

²⁶⁷ *Id.*

²⁶⁸ See Booz Allen Hamilton Comment at 17.

²⁶⁹ *Id.*

²⁷⁰ Association for Computing Machinery U.S. Policy Council Comment at 7; Nest Labs Comment at 15; 5G Americas Comment at 9-12; ACT | The App Association Comment at 11.

within the Department, domestically, and abroad, and will continue to be a champion of emerging technologies and the digital economy, as described in the examples below.

1. *Current Initiatives*

- **Census Enterprise Data Collection and Processing Initiative (CEDCaP).** The CEDCaP aims to unify more than 100 systems used in the 2010 census to a single platform by the 2020 census, allowing shared data collection and processing across all censuses and surveys. One part of this initiative is incorporation of IoT technology into the work of the 20,000 census field workers.²⁷¹
- **Skills for Business Initiative.** The Department has committed to use all of its pertinent assets to strengthen regional economies by supporting employer-led partnerships to address talent pipeline challenges, including within emerging technologies such as IoT.
- **Census Bureau Research on 1099 Form.** Recent advances in technology have changed how workers and employers interact in the 21st century labor market, and it is essential that our measures of employment and earnings evolve in order to remain accurate and relevant. To that end, the Census Bureau is conducting new research using IRS tax records from the “1099 form” for services performed by independent contractors as well as the use of contract workers at U.S. employer firms. These projects will inform how our labor market is evolving already and how our statistical system should evolve in response to a labor market that is dynamic due to developments such as the emergence of IoT.
- **The National Oceanic and Atmospheric Administration’s (NOAA) Whale Alert.** NOAA incorporates a variety of IoT sensors, provided in collaboration with many of its partners, to collect and distribute information on Earth’s environment, from local weather data to the location of whales and other marine mammals. As an example of a particular IoT data collection application, NOAA is collecting user-contributed information on Earth’s magnetic field via a free smartphone app that provides users the option to share data with the agency from a phone’s internal digital compass. The smartphone compass data is then used by NOAA scientists to construct new, more detailed models of the Earth’s varying magnetic field, which are in turn used for a wide variety of precision navigation applications in industry. This high resolution description of the magnetic field in complex areas such as cities and other developed areas would have otherwise been costly and difficult to achieve.²⁷²

²⁷¹ Grayson Ullman, Census Bureau aims to save \$5.2B with IoT and mobile tech, Fed Scoop (Nov. 4, 2015), <http://fedscoop.com/census-bureau-to-save-2-5-billion-with-iot-tech>.

²⁷² Larry O’Hanlon, Smartphone app seeks to make navigation safer, EOS (Jan. 6, 2015), <https://eos.org/articles/smartphone-app-seeks-make-navigation-safer>.

- **Commerce Data Service.** This team of designers, developers, software engineers, and data scientists works to transform raw data from the 12 bureaus, including data collected through connected devices, into insights, products, and applications to empower data-driven decision making.
- **Digital Trade Officers, Intellectual Property Attachés, and Standards Attachés.** To respond to the benefits and challenges associated with the digital economy, including IoT, the Department launched a pilot program in March 2016 for Digital Trade Officers to facilitate U.S. private sector involvement in the global digital economy and to help U.S. companies reach markets worldwide. This initiative and its pilot (launched in Brazil, China, Japan, India, the European Union, and in the Association of Southeast Asian Nations [ASEAN] region) are led by the Department's International Trade Administration (ITA), working with bureaus across the Department, in collaboration with the State Department and industry stakeholders. The Digital Trade Officers advance commercial diplomacy by driving policy advocacy on technology issues, ensure linkages between trade policy and trade promotion efforts, and provide front-line assistance for U.S. small and medium enterprises to take advantage of the robust e-commerce channels. ITA also has Standards Attachés in four U.S. embassies and consulates who are able to proactively monitor and work to address standards issues that have potential trade implications for U.S. industry and businesses.

In addition, USPTO Intellectual Property Attachés aid U.S. embassies, consulates, and international missions.²⁷³ The attachés advocate improving intellectual property policies, laws and regulations abroad, and provide information to help U.S. stakeholders entering foreign markets or conducting business abroad, including on IoT-related issues.

2. Proposed Next Steps

The Department will:

- Continue to work toward fulfilling the missions of its various bureaus with greater impact and efficiency by leveraging emerging technologies such as IoT.
- Inform and influence government practices (purchasing and otherwise) in the use of emerging technologies such as IoT in a way that maximizes efficiency and the public good while protecting the security and privacy of individuals, which will help promote a market for devices that are consistent with these practices.

²⁷³ See Intellectual Property Attaché Program, U.S. Patent and Trademark Office website, <https://www.uspto.gov/learning-and-resources/ip-policy/intellectual-property-rights-ipr-attach-program/intellectual>.

- Leverage its role as an IoT consumer to promote a market for secure IoT technologies and the supply chains supporting those technologies.
- Play an active role in 21st century skills development by inserting the business perspective into federal workforce policy making to support creation of quality career paths for workers, particularly in areas of emerging technologies such as IoT, to meet employer demand.
- Incorporate the Internet of Things into current education and awareness programs, such as the USPTO's Global Intellectual Property Academy, which provides intellectual property training in the United States and around the world.
- Explore developing metrics to better understand the role of IoT in the industrial value chain and its contributions to GDP, exports, and other economic measures. The Department will establish a definition for the digital economy and develop estimates of the domestic output, value added, and employment associated with the digital economy.
- Conduct research to improve the measurement of information and communications technology-enabled goods and services (including IoT) in order to improve the estimate of GDP, particularly as it relates to the digital economy, and productivity.

5. Conclusion

The Department recognizes the exciting promise of IoT in benefiting the lives of individuals, the economy, and society. This potential flows from a broad range of positive potential results, including increased efficiencies in industrial supply chains and systems; better use of resources through investment in Smart Cities and infrastructure; improved health and safety; and new, innovative consumer devices and possibly even as-yet-unimagined industries. Realizing these benefits will not be without obstacles, as the necessary infrastructure and policies must be in place to foster its growth while protecting individuals and society. The challenges of IoT are not all new, but in many instances are rather extensions of existing information and communication technology conversations. At the same time, IoT and its concurrent challenges are qualitatively different in that IoT increases the scale, scope, and stakes of these issues.

The approach described above is an articulation and strong affirmation of the decades-old U.S. Government approach to innovation and emerging technology, tailored to address the unique opportunities and challenges presented by IoT through the tools available to the Department of Commerce. Consistent with the values laid out in the Department's approach, our continued engagement with stakeholders is critical to crafting policy that will help to foster an innovative

IoT environment that protects individuals. Accordingly, the Department is seeking further comment on the issues discussed in this report, and intends for the comments responding to this green paper to contribute to the Department's domestic policy efforts and international engagement related to IoT.

Appendix A: Proposed Next Steps

In addition to continuing the Department's ongoing work on IoT, this green paper identifies the following next steps for the Department and its bureaus, budget and resources permitting. The Department will:

Enabling Infrastructure Availability and Access

- Coordinate with the private sector, as well as federal, state, and local government partners, to ensure the infrastructure to support IoT continues to expand, that access to infrastructure is inclusive and affordable, and that the infrastructure remains innovative, open, secure, interoperable, and stable. This includes promoting adoption and usage to encourage deployment and investment, and engaging in technical assistance and research and development.
- Continue to innovate in spectrum management to increase access to spectrum that will help facilitate IoT growth and advancement. NTIA, through its Office of Spectrum Management, will collaborate with stakeholders, including its spectrum-related interagency (Policy and Plans Steering Group and Interdepartmental Radio Advisory Committee) and external advisory bodies (Commerce Spectrum Management Advisory Committee), to assess the spectrum implications of the diverse IoT applications that currently or in the future may be delivered through a number of technologies operating in various spectrum bands.
- Expand its digital inclusion efforts to include an emphasis on IoT adoption and availability.
- Continue to encourage the adoption of IPv6 by fostering multistakeholder collaboration and dialogue, and provide a platform for discussion on issues such as mobile IPv6 routing, security in dual-stack environments, and privacy implications of IPv6.
- Collect data and conduct analysis on the usage and growth of IoT devices through its Digital Nation data collection in order to better inform industry and policy makers.

Crafting Balanced Policy and Building Coalitions

- Continue to foster an enabling environment for IoT technology to grow and thrive, allow the private sector to lead, and promote technology-neutral standards and consensus-based multistakeholder approaches to policy making at local, tribal, state, federal, and international levels on issues ranging from U.S. security and competitiveness to cybersecurity, privacy, intellectual property, the free flow of information, digital inclusion, interoperability, and stability related to IoT.

- Identify and, where appropriate, convene multistakeholder processes on IoT policy issues based on stakeholder feedback in areas such as cybersecurity, privacy, inclusion, intellectual property, and cross-border data flows.
- Proactively engage and collaborate with other relevant agencies on IoT in order to protect the safety and rights of individuals, promote innovation, and ensure a consistent and predictable regulatory environment, such as with the Department of Homeland Security,²⁷⁴ the Department of Transportation,²⁷⁵ and the Food and Drug Administration,²⁷⁶ among others.
- Leverage its country and industry experts and work closely with key interagency partners toward a consistent and predictable international IoT policy environment based on bottom-up, industry-led solutions.
- **Cybersecurity.**
 - Proactively support and promote cybersecurity policy for the IoT environment that encourages risk-based approaches, security by design, and the ability to fix or “patch” insecure software and devices.
 - As one of the key tools for addressing IoT cybersecurity concerns, promote the use of strong encryption in IoT services and products to address security concerns in the government’s risk-based approach to the use and application of IoT technologies.
 - Collaborate with industry to educate consumers on issues such as how to limit risks associated with unsecured connected devices (e.g., by changing default passwords, using password-protected home Wi-Fi networks, and employing virtual private networks).
 - On December 2nd, 2016, the Presidential Commission on Enhancing National Cybersecurity presented its report to the President, which included several recommendations specific to IoT. The Department welcomes the Commission’s endorsement of the Department’s leadership role in helping to guide cybersecurity policy, and is carefully reviewing and considering the Commission’s recommendations as we move forward in our efforts to meet the nation’s cybersecurity needs.

²⁷⁴ See <https://www.dhs.gov/securingtheIoT>

²⁷⁵ See <https://www.transportation.gov/AV>

²⁷⁶ See <http://www.fda.gov/MedicalDevices/DigitalHealth/ucm373213.htm>

- **Privacy.** Work to address the need to protect consumer privacy in the IoT environment, and continue to support baseline privacy legislation, as well as an engineering approach to privacy.
- **Intellectual Property.** Work to promote the positive evolution of intellectual property and its protection in the digital economy.
- **Cross-Border Data Flows.** Work with its international partners toward an industry-led global marketplace that promotes innovation for IoT and supports the free flow of information, and the ability of American companies to compete fairly around the world.

Promoting Standards and Technology Advancement

- Monitor IoT-related technology developments and applications and contribute to research and development involving those technologies.
- Advocate for industry-led, consensus-based, international standards for IoT technologies and applications in its bilateral and multilateral engagements.
- Actively participate in, and contribute to, the development of technical standards for IoT.

Encouraging Markets

- Continue to work toward fulfilling the missions of its various bureaus with greater impact and efficiency by leveraging emerging technologies such as IoT.
- Inform and influence government practices (purchasing and otherwise) in the use of emerging technologies such as IoT in a way that maximizes efficiency and the public good while protecting the security and privacy of individuals, which will help promote a market for devices that are consistent with these practices.
- Leverage its role as an IoT consumer to promote a market for secure IoT technologies and the supply chains supporting those technologies.
- Play an active role in 21st century skills development by inserting the business perspective into federal workforce policy making to support creation of quality career paths for workers, particularly in areas of emerging technologies such as IoT, to meet employer demand.

- Incorporate the Internet of Things into current education and awareness programs, such as USPTO's Global Intellectual Property Academy, which provides intellectual property training in the United States and around the world.
- Explore developing metrics to better understand the role of IoT in the industrial value chain and its contributions to GDP, exports, and other economic measures. The Department will establish a definition for the digital economy and develop estimates of the domestic output, value added, and employment associated with the digital economy.
- Conduct research to improve the measurement of information and communications technology-enabled goods and services (including IoT) in order to improve the estimate of GDP, particularly as it relates to the digital economy and productivity.

Appendix B: Questions for Further Discussion

This green paper is part of the Department's ongoing engagement with the public, industry, and our sister agencies on IoT. Shortly after the release of this paper, the Department will issue an additional Request for Comment presenting the following questions for further discussion and consideration by policymakers:

- 1) Is our discussion of IoT presented in the green paper regarding the challenges, benefits, and potential role of government accurate and/or complete? Are there issues that we missed, or that we need to reconsider?
- 2) Is the approach for Departmental action to advance the Internet of Things comprehensive in the areas of engagement? Where does the approach need improvement?
- 3) Are there specific tasks that the Department should engage in that are not covered by the approach?
- 4) What should the next steps be for the Department in fostering the advancement of IoT?

Appendix C: Acknowledgements, Workshop Panelists, and Request for Comment Respondents

The Digital Economy Leadership Team and Internet Policy Task Force extends its thanks to all of the individuals and organizations who participated in our public Workshop on Fostering the Advancement of the Internet of Things, and those who submitted written comments to the Notice of Inquiry that served as the basis for this report.

Workshop Panelists (as identified in the Workshop agenda):

Bridget Karlin –Intel IoT Strategy and Integrated Products

Dean Garfield –Information Technology Industry Council (ITI)

Hilary Cain –Technology and Innovation Policy, Toyota

John Godfrey –Samsung Electronics America

Sterling Rooke –X8

Kenneth Tobin – Electrical & Electronics Systems Research Division, Energy & Environmental Sciences Directorate, Oak Ridge National Laboratory

Dan Caprio – The Providence Group

Michelle De Mooy – Center for Democracy and Technology (CDT)

Harley Geiger – Rapid 7

John Kuzin – Qualcomm

Craig Spiezle – Online Trust Alliance

Kenya Wiley – Fashion Innovation Alliance

Hardik Bhatt – Department of Innovation & Technology, State of Illinois

Julie Brill – Hogan Lovells

Leonard Cali – Global Public Policy, AT&T

Cameron F. Kerry – Sidley Austin

Request for Comment Respondents

[5G Americas](#)

[ABA Section of Science & Technology Law](#)
[Access Now](#)
[ACM U.S. Public Policy Council](#)
[ACT | The App Association](#)
[AIM, Inc.](#)
[AIM North America](#)
[Alliance of Automobile Manufacturers](#)
[American National Standards Institute](#)
[Anonymous](#)
[Application Developers Alliance](#)
[ARM](#)
[Association of Global Automakers, Inc.](#)
[AT&T Services, Inc.](#)
[Booz Allen Hamilton Inc.](#)
[Bronfman, Jillisa](#)
[BSA | The Software Alliance](#)
[Bugcrowd](#)
[CA Technologies](#)
[Camp, L Jean, Henry, Ryan, Myers, Steven, Russo, Gianpaolo](#)
[Center for Data Innovation](#)
[Center for Strategic and International Studies](#)
[Cisco Systems, Inc.](#)
[Coalition for Cybersecurity Policy & Law](#)
[Common Sense Kids Action](#)
[Competitive Carriers Association](#)
[CompTIA](#)
[Computer & Communications Industry Association](#)
[Consumer Federation of America](#)
[Consumer Technology Association](#)
[Consumers Union](#)
[CTIA](#)
[Deere & Company](#)
[Duckduckgo](#)
[Direct Marketing Association](#)
[Edison Electric Institute](#)
[Electronic Frontier Foundation](#)
[Electronic Privacy Information Center](#)
[Ericsson](#)
[Family Online Safety Institute](#)
[Farance, Frank \(1\)](#)
[Farance, Frank \(2\)](#)

[Farhat, Karim](#)
[Fashion Innovation Alliance](#)
[Future of Privacy Forum](#)
[Gallagher, John](#)
[General Motors, LLC](#)
[Georgia Institute of Technology, Center for Advanced Communications Policy and
Rehabilitation Engineering Research Center for Wireless Technologies](#)
[GS1 US](#)
[GSM Association](#)
[Hewlett Packard Enterprise](#)
[Huawei Technologies, Inc.](#)
[Hughes Network Systems, LLC](#)
[IBM](#)
[IEEE-USA](#)
[Infineon Technologies Americas Corp.](#)
[Inmarsat, Inc.](#)
[InterDigital, Inc.](#)
[Internet Architecture Board](#)
[Internet Association](#)
[Internet Commerce Coalition](#)
[Internet Society](#)
[IoT Policy Network](#)
[ITI](#)
[James, Gilbert](#)
[Jones, Kim L.](#)
[Krawetz, Neal ; Schultz, Eric; Kaminsky, Valerie; Tucker, Bill; et al](#)
[Kurz, Jack](#)
[Lanting, Dr Cees J.M.](#)
[Larry, J. Christopher](#)
[LeFlore, Fannie](#)
[Ligado Networks](#)
[Local Innovation and Skill Cluster Anchor Network Project, Safe and Healthy Communities
Project/All Communities Agenda, Internet Public Trust](#)
[Louchez, Alain](#)
[Manwaring, Kayleen](#)
[Marcus, Dr Robert](#)
[Microsoft Corporation](#)
[Milne, Claire](#)
[Mobile Future](#)
[Motorola Solutions, Inc](#)
[monica2](#)

[National Association of Manufacturers](#)
[National Association of REALTORS](#)
[National Cable & Telecommunications Association](#)
[National Emergency Number Association, National Association of State 9-1-1 Administrators](#)
[Nest Labs, Inc.](#)
[NetChoice](#)
[Niskanen Center](#)
[Nokia](#)
[Online Trust Alliance](#)
[Open Connectivity Foundation](#)
[Owners' Rights Initiative](#)
[Peppet, Scott R.](#)
[Plessel, Todd](#)
[Pratt, Steve](#)
[Providence Group](#)
[Public Knowledge](#)
[Qualcomm Incorporated](#)
[Raff, John](#)
[Rapid7](#)
[Renkis, Martin A.](#)
[Rosner, Dr. Gilad L.](#)
[Samsung](#)
[Samsung \(2\)](#)
[Samsung \(3\)](#)
[Satellite Industry Association](#)
[Schoepf, Walter H.](#)
[Secure ID Coalition](#)
[Security Industry Association](#)
[Semiconductor Industry Association](#)
[Senators Schatz, Fischer, Booker, and Ayotte](#)
[Silver Spring Networks](#)
[Software & Information Industry Association](#)
[Southern Company Services, Inc.](#)
[Spiess, Tony](#)
[Staff of the Federal Trade Commission's Bureau of Consumer Protection and Office of Policy Planning](#)
[State of Illinois](#)
[Symantec](#)
[Sysorex USA](#)
[T-Mobile USA, Inc.](#)
[Telecommunications Industry Association](#)

[Thierer, Adam](#)

[Tim - The “Oldcommguy\(tm\)”](#)

[Trans-Atlantic Business Council](#)

[Tribl](#)

[University Corporation for Advanced Internet Development \(d/b/a “Internet2”\)](#)

[University of Michigan](#)

[U.S. Chamber of Commerce Center for Advanced Technology and Innovation](#)

[U.S. Council for International Business](#)

[United States Telecom Association](#)

[Verizon](#)

[Visa Inc.](#)

[Vodafone US Inc. \(12.7 MB\)](#)

[Walters, Riley](#)

[Wi-Fi Alliance](#)

[Withrow, Scott C.](#)

[Wireless Infrastructure Association](#)

[Zebra Technologies Corporation](#)

The FTC's Endorsement Guides

What People Are Asking



Contents

About the Endorsement Guides	3
When Does the FTC Act Apply to Endorsements?.....	4
Product Placements.....	8
Endorsements by Individuals on Social Networking Sites	9
How Should I Disclose That I Was Given Something for My Endorsement? ...	10
Other Things for Endorsers to Know	13
Social Media Contests.....	14
Online Review Programs.....	14
Soliciting Endorsements	15
What Are an Advertiser’s Responsibilities for What Others Say in Social Media?	16
What About Intermediaries?.....	17
What About Affiliate or Network Marketing?.....	18
Expert Endorsers Making Claims Outside of Traditional Advertisements	19
Employee Endorsements	20
Using Testimonials That Don’t Reflect the Typical Consumer Experience.....	21
Where can I find out more?	22
Your Opportunity to Comment.....	22

Suppose you meet someone who tells you about a great new product. She tells you it performs wonderfully and offers fantastic new features that nobody else has. Would that recommendation factor into your decision to buy the product? Probably.

Now suppose the person works for the company that sells the product – or has been paid by the company to tout the product. Would you want to know that when you're evaluating the endorser's glowing recommendation? You bet. That common-sense premise is at the heart of the Federal Trade Commission's (FTC) Endorsement Guides.

The Guides, at their core, reflect the basic truth-in-advertising principle that endorsements must be honest and not misleading. An endorsement must reflect the honest opinion of the endorser and can't be used to make a claim that the product's marketer couldn't legally make.

In addition, the Guides say if there's a connection between an endorser and the marketer that consumers would not expect and it would affect how consumers evaluate the endorsement, that connection should be disclosed. For example, if an ad features an endorser who's a relative or employee of the marketer, the ad is misleading unless the connection is made clear. The same is usually true if the endorser has been paid or given something of value to tout the product. The reason is obvious: Knowing about the connection is important information for anyone evaluating the endorsement.

Say you're planning a vacation. You do some research and find a glowing review on someone's blog that a particular resort is the most luxurious place he has ever stayed. If you knew the hotel had paid the blogger hundreds of dollars to say great things about it or that the blogger had stayed there for several days for free, it could affect how much weight you'd give the blogger's endorsement. The blogger should, therefore, let his readers know about that relationship.

Another principle in the Guides applies to ads that feature endorsements from people who achieved exceptional, or even above average, results. An example is an endorser who says she lost 20 pounds in two months using the advertised product. If the advertiser doesn't have proof that the endorser's experience represents what people will generally achieve using the product as described in the ad (for example, by just taking a pill daily for two months), then an ad featuring that endorser must make clear to the audience what the generally expected results are.

Here are answers to some of our most frequently asked questions from advertisers, ad agencies, bloggers, and others.

About the Endorsement Guides

Do the Endorsement Guides apply to social media?

Yes. Truth in advertising is important in all media, whether they have been around for decades (like, television and magazines) or are relatively new (like, blogs and social media).

Isn't it common knowledge that bloggers are paid to tout products or that if you click a link on a blogger's site to buy a product, the blogger will get a commission?

No. Some bloggers who mention products in their posts have no connection to the marketers of those products – they don't receive anything for their reviews or get a commission. They simply recommend those products to their readers because they believe in them.

Moreover, the financial arrangements between some bloggers and advertisers may be apparent to industry insiders, but not to everyone else who reads a particular blog. Under the law, an act or practice is deceptive if it misleads "a significant minority" of consumers. Even if some readers are aware of these deals, many readers aren't. That's why disclosure is important.

Are you monitoring bloggers?

Generally not, but if concerns about possible violations of the FTC Act come to our attention, we'll evaluate them case by case. If law enforcement becomes necessary, our focus usually will be on advertisers or their ad agencies and public relations firms. Action against an individual endorser, however, might be appropriate in certain circumstances.

Does the FTC hold online reviewers to a higher standard than reviewers for paper-and-ink publications?

No. The FTC Act applies across the board. The issue is – and always has been – whether the audience understands the reviewer's relationship to the company whose products are being recommended. If the audience understands the relationship, a disclosure isn't needed.

If you're employed by a newspaper or TV station to give reviews – whether online or offline – your audience probably understands that your job is to provide your personal opinion on behalf of the newspaper or television station. In that situation, it's clear that you did not buy the product yourself – whether it's a book or a car or a movie ticket. On a personal blog, a social networking page, or in similar media, the reader might not

realize that the reviewer has a relationship with the company whose products are being recommended. Disclosure of that relationship helps readers decide how much weight to give the review.

What is the legal basis for the Guides?

If an endorser is acting on behalf of an advertiser, what she or he is saying is usually going to be commercial speech – and commercial speech violates the FTC Act if it's deceptive. The FTC conducts investigations and brings cases involving endorsements under Section 5 of the FTC Act, which generally prohibits deceptive advertising.

The Guides are intended to give insight into what the FTC thinks about various marketing activities involving endorsements and how Section 5 might apply to those activities. The Guides themselves don't have the force of law. However, practices inconsistent with the Guides may result in law enforcement actions for violations of the FTC Act. Although there are no fines for violations of the FTC Act, law enforcement actions can result in orders requiring the defendants in the case to give up money they received from their violations.

When Does the FTC Act Apply to Endorsements?

I'm a blogger. I heard that every time I mention a product on my blog, I have to say whether I got it for free or paid for it myself. Is that true?

No. If you mention a product you paid for yourself, there isn't an issue. Nor is it an issue if you get the product for free because a store is giving out free samples to its customers.

The FTC is only concerned about endorsements that are made on behalf of a sponsoring advertiser. For example, an endorsement would be covered by the FTC Act if an advertiser – or someone working for an advertiser – pays you or gives you something of value to mention a product. If you receive free products or other perks with the expectation that you'll promote or discuss the advertiser's products in your blog, you're covered. Bloggers who are part of network marketing programs where they sign up to receive free product samples in exchange for writing about them also are covered.

What if all I get from a company is a \$1-off coupon, an entry in a sweepstakes or a contest, or a product that is only worth a few dollars? Does that still have to be disclosed?

The question you need to ask is whether knowing about that gift or incentive would affect the weight or credibility your readers give to your recommendation. If it could, then it should be disclosed. For example, being entered into a sweepstakes or a contest for a

chance to win a thousand dollars in exchange for an endorsement could very well affect how people view that endorsement. Determining whether a small gift would affect the weight or credibility of an endorsement could be difficult. It's always safer to disclose that information.

Also, even if getting one free item that's not very valuable doesn't affect your credibility, continually getting free stuff from an advertiser or multiple advertisers could suggest you expect future benefits from positive reviews. If a blogger or other endorser has a relationship with a marketer or a network that sends freebies in the hope of positive reviews, it's best to let readers know about the free stuff.

Even an incentive with no financial value might affect the credibility of an endorsement and would need to be disclosed. The Guides give the example of a restaurant patron being offered the opportunity to appear in television advertising before giving his opinion about a product. Because the chance to appear in a TV ad could sway what someone says, that incentive should be disclosed.

What if I upload a video to YouTube that shows me reviewing several products? Should I disclose when I got them from an advertiser?

Yes. The guidance for videos is the same as for websites or blogs.

What if I return the product after I review it? Should I still make a disclosure?

That might depend on the product and how long you are allowed to use it. For example, if you get free use of a car for a month, we recommend a disclosure even though you have to return it. But even for less valuable products, it's best to be open and transparent with your readers.

I have a website that reviews local restaurants. It's clear when a restaurant pays for an ad on my website, but do I have to disclose which restaurants give me free meals?

If you get free meals, you should let your readers know so they can factor that in when they read your reviews. Some readers might conclude that if a restaurant gave you a free meal because it knew you were going to write a review, you might have gotten special food or service.

Several months ago a manufacturer sent me a free product and asked me to write about it in my blog. I tried the product, liked it, and wrote a favorable review. When I posted the review, I disclosed that I got the product for free from the manufacturer. I still use the product. Do I have to disclose that I got the product for free every time I mention it in my blog?

It might depend on what you say about it, but each new endorsement made without a disclosure could be deceptive because readers might not see the original blog post where you said you got the product free from the manufacturer.

A trade association hired me to be its “ambassador” and promote its upcoming conference in social media, primarily on Facebook, Twitter, and in my blog. The association is only hiring me for five hours a week. I disclose my relationship with the association in my blogs and in the tweets and posts I make about the event during the hours I’m working. But sometimes I get questions about the conference in my off time. If I respond via Twitter when I’m not officially working, do I need to make a disclosure? Can that be solved by placing a badge for the conference in my Twitter profile?

You have a financial connection to the company that hired you and that relationship exists whether or not you are being paid for a particular tweet. If you are endorsing the conference in your tweets, your audience has a right to know about your relationship. That said, some of your tweets responding to questions about the event might not be endorsements, because they aren’t communicating your opinions about the conference (for example, if someone just asks you for a link to the conference agenda).

Also, if you respond to someone’s questions about the event via email or text, that person probably already knows your affiliation or they wouldn’t be asking you. You probably wouldn’t need a disclosure in that context. But when you respond via social media, all your followers see your posts and some of them might not have seen your earlier disclosures.

With respect to posting the conference’s badge on your Twitter profile page, a disclosure on a profile page isn’t sufficient because many people in your audience probably won’t see it. Also, depending upon what it says, the badge may not adequately inform consumers of your connection to the trade association. If it’s simply a logo or hashtag for the event, it won’t tell consumers of your relationship to the association.

I share in my social media posts about products I use. Do I actually have to say something positive about a product for my posts to be endorsements covered by the FTC Act?

Simply posting a picture of a product in social media, such as on Pinterest, or a video of you using it could convey that you like and approve of the product. If it does, it's an endorsement.

You don't necessarily have to use words to convey a positive message. If your audience thinks that what you say or otherwise communicate about a product reflects your opinions or beliefs about the product, and you have a relationship with the company marketing the product, it's an endorsement subject to the FTC Act.

Of course, if you don't have any relationship with the advertiser, then your posts simply are not subject to the FTC Act, no matter what you show or say about the product. The FTC Act covers only endorsements made on behalf of a sponsoring advertiser.

My Facebook page identifies my employer. Should I include an additional disclosure when I post on Facebook about how useful one of our products is?

It's a good idea. People reading your posts in their news feed – or on your profile page – might not know where you work or what products your employer makes. Many businesses are so diversified that readers might not realize that the products you're talking about are sold by your company.

A famous athlete has thousands of followers on Twitter and is well-known as a spokesperson for a particular product. Does he have to disclose that he's being paid every time he tweets about the product?

It depends on whether his followers understand that he's being paid to endorse that product. If they know he's a paid endorser, no disclosure is needed. But if a significant portion of his followers don't know that, the relationship should be disclosed. Determining whether followers are aware of a relationship could be tricky in many cases, so we recommend disclosure.

A famous celebrity has millions of followers on Twitter. Many people know that she regularly charges advertisers to mention their products in her tweets. Does she have to disclose when she's being paid to tweet about products?

It depends on whether her followers understand that her tweets about products are paid endorsements. If a significant portion of her followers don't know that, disclosures are needed. Again, determining that could be tricky, so we recommend disclosure.

Product Placements

What does the FTC have to say about product placements on television shows?

Federal Communications Commission (FCC, not FTC) law requires TV stations to include disclosures of product placement in TV shows.

FTC staff has expressed the opinion that under the FTC Act, product placement (that is, merely showing products or brands in third-party entertainment or news content – as distinguished from sponsored content or disguised commercials), doesn't require a disclosure that the placement was paid-for by the advertiser.

What if the host of a television talk show expresses her opinions about a product – let's say a videogame – and she was paid for the promotion? The segment is entertainment, it's humorous, and it's not like the host is an expert. Is that different from a product placement and does the payment have to be disclosed?

If the host endorses the product – even if she is just playing the game and saying something like “wow, this is awesome” – it's more than a product placement. If the payment for the endorsement isn't expected by the audience and it would affect the weight the audience gives the endorsement, it should be disclosed. It doesn't matter that the host isn't an expert or the segment is humorous as long as the endorsement has credibility that would be affected by knowing about the payment. However, if what the host says is obviously an advertisement – think of an old-time television show where the host goes to a different set, holds up a cup of coffee, says “Wake up with ABC Coffee. It's how I start my day!” and takes a sip – a disclosure probably isn't necessary.

Endorsements by Individuals on Social Networking Sites

Many social networking sites allow you to share your interests with friends and followers by clicking a button or sharing a link to show that you're a fan of a particular business, product, website or service. Is that an "endorsement" that needs a disclosure?

Many people enjoy sharing their fondness for a particular product or service with their social networks.

If you write about how much you like something you bought on your own and you're not being rewarded, you don't have to worry. However, if you're doing it as part of a sponsored campaign or you're being compensated – for example, getting a discount on a future purchase or being entered into a sweepstakes for a significant prize – then a disclosure is appropriate.

I am an avid social media user who often gets rewards for participating in online campaigns on behalf of brands. Is it OK for me to click a "like" button, pin a picture, or share a link to show that I'm a fan of a particular business, product, website or service as part of a paid campaign?

Using these features to endorse a company's products or services as part of a sponsored brand campaign probably requires a disclosure.

We realize that some platforms – like Facebook's "like" buttons – don't allow you to make a disclosure. Advertisers shouldn't encourage endorsements using features that don't allow for clear and conspicuous disclosures. However, we don't know at this time how much stock social network users put into "likes" when deciding to patronize a business, so the failure to disclose that the people giving "likes" received an incentive might not be a problem.

An advertiser buying fake "likes" is very different from an advertiser offering incentives for "likes" from actual consumers. If "likes" are from non-existent people or people who have no experience using the product or service, they are clearly deceptive, and both the purchaser and the seller of the fake "likes" could face enforcement action.

I posted a review of a service on a website. Now the marketer has taken my review and changed it in a way that I think is misleading. Am I liable for that? What can I do?

No, you aren't liable for the changes the marketer made to your review. You could, and probably should, complain to the marketer and ask them to stop using your altered review. You also could file complaints with the FTC, your local consumer protection organization, and the Better Business Bureau.

How Should I Disclose That I Was Given Something for My Endorsement?

Is there special wording I have to use to make the disclosure?

No. The point is to give readers the essential information. A simple disclosure like "Company X gave me this product to try" will usually be effective.

Do I have to hire a lawyer to help me write a disclosure?

No. What matters is effective communication, not legalese. A disclosure like "Company X sent me [name of product] to try, and I think it's great" gives your readers the information they need. Or, at the start of a short video, you might say, "Some of the products I'm going to use in this video were sent to me by their manufacturers." That gives the necessary heads-up to your viewers.

When should I say more than that I got a product for free?

It depends on what else (if anything) you received from the company.

For example, if an app developer gave you their 99-cent app for free in order for you to review it, that might not have much effect on the weight that readers give to your review. But if the app developer also gave you \$100, that would have a much greater effect on the credibility of your review. So a disclosure that simply said you got the app for free wouldn't be good enough.

Similarly, if a company gave you a \$50 gift card to give away to one of your readers and a second \$50 gift card to keep for yourself, it wouldn't be good enough to only say that the company gave you a gift card to give away.

I'm doing a review of a videogame that hasn't been released yet. The manufacturer is paying me to try the game and review it. I was planning on disclosing that the manufacturer gave me a "sneak peak" of the game. Isn't that enough to put people on notice of my relationship to the manufacturer?

No, it's not. Getting early access doesn't mean that you got paid. Getting a "sneak peak" of the game doesn't even mean that you get to keep the game. If you get early access, you can say that, but if you are paid, you should say so.

Are you saying that I need to list the details of everything I get from a company for reviewing a product?

No. As long as your audience knows the nature of your relationship, it's good enough. So whether you got \$50 or \$1,000 you could simply say you were "paid." (That wouldn't be good enough, however, if you're an employee or co-owner.)

Would a single disclosure on my home page that "many of the products I discuss on this site are provided to me free by their manufacturers" be enough?

A single disclosure on your home page doesn't really do it because people visiting your site might read individual reviews or watch individual videos without seeing the disclosure on your home page.

If I upload a video to YouTube and that video requires a disclosure, can I just put the disclosure in the description that I upload together with the video?

No, because it's easy for consumers to miss disclosures in the video description. Many people might watch the video without even seeing the description page, and those who do might not read the disclosure. The disclosure has the most chance of being effective if it is made clearly and prominently in the video itself. That's not to say that you couldn't have disclosures in both the video and the description.

Would a button that says DISCLOSURE, LEGAL, or something like that which links to a full disclosure be sufficient?

No. A hyperlink like that isn't likely to be sufficient. It does not convey the importance, nature, and relevance of the information to which it leads and it is likely that many consumers will not click on it and therefore miss necessary disclosures. The disclosures we are talking about are brief and there is no reason to hide them behind a hyperlink.

What about a platform like Twitter? How can I make a disclosure when my message is limited to 140 characters?

The FTC isn't mandating the specific wording of disclosures. However, the same general principle – that people get the information they need to evaluate sponsored statements – applies across the board, regardless of the advertising medium. The words “Sponsored” and “Promotion” use only 9 characters. “Paid ad” only uses 7 characters. Starting a tweet with “Ad:” or “#ad” – which takes only 3 characters – would likely be effective.

The Guides say that disclosures have to be clear and conspicuous. What does that mean?

To make a disclosure “clear and conspicuous,” advertisers should use clear and unambiguous language and make the disclosure stand out. Consumers should be able to notice the disclosure easily. They should not have to look for it. In general, disclosures should be:

- close to the claims to which they relate;
- in a font that is easy to read;
- in a shade that stands out against the background;
- for video ads, on the screen long enough to be noticed, read, and understood;
- for audio disclosures, read at a cadence that is easy for consumers to follow and in words consumers will understand.

A disclosure that is made in both audio and video is more likely to be noticed by consumers. Disclosures should not be hidden or buried in footnotes, in blocks of text people are not likely to read, or in hyperlinks. If disclosures are hard to find, tough to understand, fleeting, or buried in unrelated details, or if other elements in the ad or message obscure or distract from the disclosures, they don't meet the “clear and conspicuous” standard. With respect to online disclosures, FTC staff has issued a guidance document, “.com Disclosures: How to Make Effective Disclosures in Digital Advertising,” which is available on ftc.gov.

I've been paid to endorse a product in social media. My posts, videos, and tweets will be in Spanish. In what language should I disclose that I've been paid for the promotion?

The connection between an endorser and a marketer should be disclosed in whatever language or languages the endorsement is made, so your disclosures should be in Spanish.

I guess I need to make a disclosure that I've gotten paid for a video review that I'm uploading to YouTube. When in the review should I make the disclosure? Is it ok if it's at the end?

It's more likely that a disclosure at the end of the video will be missed, especially if someone doesn't watch the whole thing. Having it at the beginning of the review would be better. Having multiple disclosures during the video would be even better. Of course, no one should promote a link to your review that bypasses the beginning of the video and skips over the disclosure. If YouTube has been enabled to run ads during your video, a disclosure that is obscured by ads is not clear and conspicuous.

I'm getting paid to do a videogame playthrough and give commentary while I'm playing. The playthrough – which will last several hours – will be live streamed. Would a disclosure at the beginning of the stream be ok?

Since viewers can tune in any time, they could easily miss a disclosure at the beginning of the stream or at any other single point in the stream. People should see a disclosure no matter when they tune in. There could be multiple, periodic disclosures throughout the stream. To be cautious, you could have a continuous, clear and conspicuous disclosure throughout the entire stream.

Other Things for Endorsers to Know

Besides disclosing my relationship with the company whose product I'm endorsing, what are the essential things I need to know about endorsements?

The most important principle is that an endorsement has to represent the accurate experience and opinion of the endorser:

- You can't talk about your experience with a product if you haven't tried it.
- If you were paid to try a product and you thought it was terrible, you can't say it's terrific.

You can't make claims about a product that would require proof the advertiser doesn't have. The Guides give the example of a blogger commissioned by an advertiser to review a new body lotion. Although the advertiser does not make any claims about the lotion's ability to cure skin conditions and the blogger does not ask the advertiser whether there is substantiation for the claim, she writes that the lotion cures eczema. The blogger is subject to liability for her unsubstantiated claims.

Social Media Contests

My company runs contests and sweepstakes in social media. To enter, participants have to send a Tweet or make a pin with the hashtag, #XYZ_Rocks. (“XYZ” is the name of my product.) Isn’t that enough to notify readers that the posts were incentivized?

No, it is likely that many readers would not understand such a hashtag to mean that those posts were made as part of a contest or that the people doing the posting had received something of value (in this case, a chance to win the contest prize). Making the word “contest” or “sweepstakes” part of the hashtag should be enough. However, the word “sweeps” probably isn’t, because it is likely that many people would not understand what that means.

Online Review Programs

My company runs a retail website that includes customer reviews of the products we sell. We believe honest reviews help our customers and we give out free products to a select group of our customers for them to review. We tell them to be honest, whether it’s positive or negative. What we care about is how helpful the reviews are. Do we still need to disclose which reviews were of free products?

Yes. Knowing that reviewers got the product they reviewed for free would probably affect the weight your customers give to the reviews, even if you didn’t intend for that to happen. And even assuming the reviewers in your program are unbiased, your customers have the right to know which reviewers were given products for free. It’s also possible that the reviewers may wonder whether your company would stop sending them products if they wrote several negative reviews – despite your assurances that you only want their honest opinions – and that could affect their reviews.

My company, XYZ, operates one of the most popular multi-channel networks on YouTube. We just entered into a contract with a videogame marketer to pay some of our network members to produce and upload video reviews of the marketer's games. We're going to have these reviewers announce at the beginning of each video (before the action starts) that it's "sponsored by XYZ" and also have a prominent simultaneous disclosure on the screen saying the same thing. Is that good enough?

Many consumers could think that XYZ is a neutral third party and won't realize from your disclosures that the review was really sponsored (and paid for) by the videogame marketer, which has a strong interest in positive reviews. If the disclosure said, "Sponsored by [name of the game company]," that would be good enough.

Soliciting Endorsements

My company wants to contact customers and interview them about their experiences with our service. If we like what they say about our service, can we ask them to allow us to quote them in our ads? Can we pay them for letting us use their endorsements?

Yes, you can ask your customers about their experiences with your product and feature their comments in your ads. If they have no reason to expect compensation or any other benefit before they give their comments, there's no need to disclose your payments to them.

However, if you've given these customers a reason to expect a benefit from providing their thoughts about your product, you should disclose that fact in your ads. For example, if customers are told in advance that their comments might be used in advertising, they might expect to receive a payment for a positive review, and that could influence what they say, even if you tell them that you want their honest opinion. In fact, even if you tell your customers that you aren't going to pay them but that they might be featured in your advertising, that opportunity might be seen as having a value, so the fact that they knew this when they gave the review should be disclosed (e.g., "Customers were told in advance they might be featured in an ad.").

I'm starting a new Internet business. I don't have any money for advertising, so I need publicity. Can I tell people that if they say good things about my business in online reviews, I'll give them a discount on items they buy through my website?

It's not a good idea. Endorsements must reflect the honest opinions or experiences of the endorser, and your plan could cause people to make up positive reviews even if they've never done business with you. However, it's okay to invite people to post reviews of your business after they've actually used your products or services. If you're offering them something of value in return for these reviews, tell them in advance that they should disclose what they received from you. You should also inform potential reviewers that the discount will be conditioned upon their making the disclosure. That way, other consumers can decide how much stock to put in those reviews.

What Are an Advertiser's Responsibilities for What Others Say in Social Media?

Our company uses a network of bloggers and other social media influencers to promote our products. We understand we're responsible for monitoring our network. What kind of monitoring program do we need? Will we be liable if someone in our network says something false about our product or fails to make a disclosure?

Advertisers need to have reasonable programs in place to train and monitor members of their network. The scope of the program depends on the risk that deceptive practices by network participants could cause consumer harm – either physical injury or financial loss. For example, a network devoted to the sale of health products may require more supervision than a network promoting, say, a new fashion line. Here are some elements every program should include:

1. Given an advertiser's responsibility for substantiating objective product claims, explain to members of your network what they can (and can't) say about the products – for example, a list of the health claims they can make for your products;
2. Instruct members of the network on their responsibilities for disclosing their connections to you;
3. Periodically search for what your people are saying; and
4. Follow up if you find questionable practices.

It's unrealistic to expect you to be aware of every single statement made by a member of your network. But it's up to you to make a reasonable effort to know what participants in your network are saying. That said, it's unlikely that the activity of a rogue blogger would

be the basis of a law enforcement action if your company has a reasonable training and monitoring program in place.

Our company’s social media program is run by our public relations firm. We tell them to make sure that what they and anyone they pay on our behalf do complies with the FTC’s Guides. Is that good enough?

Your company is ultimately responsible for what others do on your behalf. You should make sure your public relations firm has an appropriate program in place to train and monitor members of its social media network. Ask for regular reports confirming that the program is operating properly and monitor the network periodically. Delegating part of your promotional program to an outside entity doesn’t relieve you of responsibility under the FTC Act.

What About Intermediaries?

I have a small network marketing business. Advertisers pay me to distribute their products to members of my network who then try the product for free. How do the principles in the Guides affect me?

You should tell the participants in your network that if they endorse products they have received through your program, they should make it clear they got them for free. Advise your clients – the advertisers – that if they provide free samples directly to your members, they should remind them of the importance of disclosing the relationship when they talk about those products. Put a program in place to check periodically whether your members are making those disclosures, and to deal with anyone who isn’t complying.

My company recruits “influencers” for marketers who want them to endorse their products. We pay and direct the influencers. What are our responsibilities?

Because of your role in recruiting and directing the influencers, your company is responsible for any failures by the influencers you pay to adequately disclose that they received payments for their endorsements. Teach your influencers to adequately disclose their compensation for endorsements and take reasonable steps to monitor their compliance with that obligation.

What About Affiliate or Network Marketing?

I'm an affiliate marketer with links to an online retailer on my website. When people read what I've written about a particular product and then click on those links and buy something from the retailer, I earn a commission from the retailer. What do I have to disclose? Where should the disclosure be?

If you disclose your relationship to the retailer clearly and conspicuously on your site, readers can decide how much weight to give your endorsement.

In some instances – like when the affiliate link is embedded in your product review – a single disclosure may be adequate. When the review has a clear and conspicuous disclosure of your relationship and the reader can see both the review containing that disclosure and the link at the same time, readers have the information they need. You could say something like, “I get commissions for purchases made through links in this post.” But if the product review containing the disclosure and the link are separated, readers may lose the connection.

As for where to place a disclosure, the guiding principle is that it has to be clear and conspicuous. The closer it is to your recommendation, the better. Putting disclosures in obscure places – for example, buried on an ABOUT US or GENERAL INFO page, behind a poorly labeled hyperlink or in a “terms of service” agreement – isn't good enough. Neither is placing it below your review or below the link to the online retailer so readers would have to keep scrolling after they finish reading. Consumers should be able to notice the disclosure easily. They shouldn't have to hunt for it.

Is “affiliate link” by itself an adequate disclosure? What about a “buy now” button?

Consumers might not understand that “affiliate link” means that the person placing the link is getting paid for purchases through the link. Similarly, a “buy now” button would not be adequate.

I hear what you're saying, but I don't just review a product here and there. My site reviews all of the products in a product category and for each product – whether we love it or pan it – I have a link to the website of a leading online retailer. I don't favor one product over another based upon my affiliate payments from the retailer. Do I really need to disclose my relationship with the retailer?

You are endorsing the specific online retailer to whom you are linking. Knowing that you are getting paid if they buy an item from that retailer, rather than from another one, might affect the weight that readers give your endorsement of the retailer.

What if I'm including links to product marketers or to retailers as a convenience to my readers, but I'm not getting paid for them?

Then there isn't anything to disclose.

Does this guidance about affiliate links apply to links in my product reviews on someone else's website, to my user comments, and to my tweets?

Yes, the same guidance applies anytime you endorse a product and get paid through affiliate links.

It's clear that what's on my website is a paid advertisement, not my own endorsement or review of the product. Do I still have to disclose that I get a commission if people click through my website to buy the product?

If it's clear that what's on your site is a paid advertisement, you don't have to make additional disclosures. Just remember that what's clear to you may not be clear to everyone visiting your site, and the FTC evaluates ads from the perspective of reasonable consumers.

Expert Endorsers Making Claims Outside of Traditional Advertisements

One of our company's paid spokespersons is an expert who appears on news and talk shows promoting our product, sometimes along with other products she recommends based on her expertise. Your Guides give an example of a celebrity spokesperson appearing on a talk show and recommend that the celebrity disclose her connection to the company she is promoting. Does that principle also apply to expert endorsers?

Yes, it does. Your spokesperson should disclose her connection when promoting your products outside of traditional advertising media (in other words, on programming that consumers won't recognize as paid advertising). The same guidance also would apply to comments by the expert in her blog or on her website.

Employee Endorsements

I work for a terrific company. Can I mention our products to people in my social networks? How about on a review site? My friends won't be misled since it's clear in my online profiles where I work.

First, we recommend that you check with your employer to make sure you're complying with its policies before using any form of social media to talk about the company's products.

If your company allows employees to use social media to talk about its products, you should make sure that your relationship is disclosed to people who read your online postings about your company or its products. Put yourself in the reader's shoes. Isn't the employment relationship something you would want to know before relying on someone else's endorsement? Listing your employer on your profile page isn't enough. After all, people who just read what you post on a review site won't get that information.

People reading your posting on a review site probably won't know who you are. You definitely should disclose your employment relationship when making an endorsement.

Our company's policy says that employees should not post positive reviews online about our products without clearly disclosing their relationship to the company. All of our employees agree to abide by this policy when they are hired. But we have several thousand people working here and we can't monitor what they all do on their own computers and other devices when they aren't at work. Are we liable if an employee posts a review of one of our products, either on our company website or on a social media site and doesn't disclose that relationship?

It wouldn't be reasonable to expect you to monitor every social media posting by all of your employees. However, you should establish a formal program to remind employees periodically of your policy, especially if the company encourages employees to share their opinions about your products. Also, if you learn that an employee has posted a review on the company's website or a social media site without adequately disclosing his or her relationship to the company, you should remind them of your company policy and ask them to remove that review or adequately disclose that they're an employee.

What about employees of an ad agency or public relations firm? Can my agency ask our employees to spread the buzz about our clients' products?

First, an ad agency (or any company for that matter) shouldn't ask employees to say anything that isn't true. No one should endorse a product they haven't used or say things they don't believe, and an employer certainly shouldn't encourage employees to do that.

Moreover, employees of an ad agency or public relations firm have a connection to the advertiser, which should be disclosed in all social media posts. Agencies asking their employees to spread the word must instruct those employees about their responsibilities to disclose their relationship.

Using Testimonials That Don't Reflect the Typical Consumer Experience

We want to run ads featuring endorsements from consumers who achieved the best results with our company's product. Can we do that?

Testimonials claiming specific results usually will be interpreted to mean that the endorser's experience reflects what others can also expect. Statements like "Results not typical" or "Individual results may vary" won't change that interpretation. That leaves advertisers with two choices:

1. Have adequate proof to back up the claim that the results shown in the ad are typical, or
2. Clearly and conspicuously disclose the generally expected performance in the circumstances shown in the ad.

How would this principle about testimonialists who achieved exceptional results apply in a real ad?

The Guides include several examples with practical advice on this topic. One example is about an ad in which a woman says, "I lost 50 pounds in 6 months with WeightAway." If consumers can't generally expect to get those results, the ad should say how much weight consumers can expect to lose in similar circumstances – for example, "Most women who use WeightAway for six months lose at least 15 pounds."

Our company website includes testimonials from some of our more successful customers who used our product during the past few years and mentions the results they got. We can't figure out now what the "generally expected results" were back then. What should we do? Do we have to remove those testimonials?

There are two issues here. First, according to the Guides, if your website says or implies that the endorser currently uses the product in question, you can use that endorsement only as long as you have good reason to believe the endorser does still use the product. If you're using endorsements that are a few years old, it's your obligation to make sure the claims still are accurate. If your product has changed, it's best to get new endorsements.

Second, if your product is the same as it was when the endorsements were given and the claims are still accurate, you probably can use the old endorsements if the disclosures are consistent with what the generally expected results are now.

Where can I find out more?

The Guides offer more than 35 examples involving various endorsement scenarios. Questions? Send them to endorsements@ftc.gov. We may address them in future FAQs.

The FTC works to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them. To file a complaint or get free information on consumer issues, visit ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. Watch a video, How to File a Complaint, at consumer.ftc.gov/media to learn more. The FTC enters consumer complaints into the Consumer Sentinel Network, a secure online database and investigative tool used by hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

Your Opportunity to Comment

The National Small Business Ombudsman and 10 Regional Fairness Boards collect comments from small businesses about federal compliance and enforcement activities. Each year, the Ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses. Small businesses can comment to the Ombudsman without fear of reprisal. To comment, call toll-free 1-888-REGFAIR (1-888-734-3247) or go to www.sba.gov/ombudsman.





United States of America
 FEDERAL TRADE COMMISSION
 Washington, D.C. 20580

Division of Advertising Practices

Mary K. Engle
 Associate Director

March 20, 2014

Christie Grymes Thompson, Esq.
 Kelley Drye & Warren LLP
 3050 K Street, NW
 Washington Harbour, Suite 400
 Washington, D.C. 20007-5108

Re: Cole Haan, FTC File No. 142-3041

Dear Ms. Thompson:

As you know, the staff of the Federal Trade Commission's Division of Advertising Practices has conducted an investigation into whether your client, Cole Haan, Inc., violated Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, in connection with its Wandering Sole Pinterest Contest.

The contest rules instructed contestants to create Pinterest¹ boards titled "Wandering Sole." The contest rules further required that a board include five shoe images from Cole Haan's Wandering Sole Pinterest Board as well as five images of the contestants' "favorite places to wander." Finally, contestants were instructed to use "#WanderingSole" in each pin description. Cole Haan promised to award a \$1,000 shopping spree to the contestant with the most creative entry.

We believe that participants' pins featuring Cole Haan products were endorsements of the Cole Haan products, and the fact that the pins were incentivized by the opportunity to win a \$1000 shopping spree would not reasonably be expected by consumers who saw the pins. Moreover, we were concerned that Cole Haan did not instruct contestants to label their pins and Pinterest boards to make it clear that they had pinned Cole Haan products as part of a contest. We do not believe that the "#WanderingSole" hashtag adequately communicated the financial incentive – a material connection – between contestants and Cole Haan.

¹ Pinterest is a social media site where users can save and organize images known as "pins" in collections known as "boards." Pinterest users may "follow" other Pinterest users, and the Pinterest home page displays a chronological "feed" of pins from boards and pinners that the user has chosen to follow. Also, users can run searches for pins by entering search terms. All Pinterest boards are public by default.

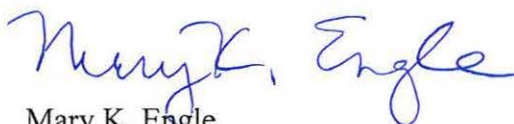
Christie Grymes Thompson, Esq.
March 20, 2014
Page 2

Section 5 of the FTC Act requires the disclosure of a material connection between a marketer and an endorser when their relationship is not otherwise apparent from the context of the communication that contains the endorsement. Under the circumstances set out above, entry into a contest to receive a significant prize in exchange for endorsing a product through social media constitutes a material connection that would not reasonably be expected by viewers of the endorsement.

Upon review of this matter, we have determined not to recommend enforcement action at this time. We considered a number of factors in reaching this decision. First, we have not previously publicly addressed whether entry into a contest is a form of material connection, nor have we explicitly addressed whether a pin on Pinterest may constitute an endorsement. Second, the contest ran for a limited length of time and drew a relatively small number of contestants. Finally, Cole Haan has since adopted a social media policy that adequately addresses our concerns. The FTC staff expects that Cole Haan will take reasonable steps to monitor social media influencers' compliance with the obligation to disclose material connections when endorsing its products.

Our decision not to pursue enforcement action is not to be construed as a determination that a violation may not have occurred, just as the pendency of an investigation should not be construed as a determination that a violation has occurred. The Commission reserves the right to take further action as the public interest may warrant.

Very truly yours,



Mary K. Engle
Associate Director for Advertising Practices

Lord & Taylor Settles FTC Charges It Deceived Consumers Through Paid Article in an Online Fashion Magazine and Paid Instagram Posts by 50 “Fashion Influencers”

Promotions Were Part of the Company’s March 2015 Design Lab Collection Launch

National retailer [Lord & Taylor](#) has agreed to settle Federal Trade Commission charges that it [deceived consumers](#) by paying for native advertisements, including a seemingly objective article in the online publication *Nylon* and a *Nylon* Instagram post, without disclosing that the posts actually were paid promotions for the company’s 2015 Design Lab clothing collection.

The [Commission’s complaint](#) also charges that as part of the Design Lab rollout, Lord & Taylor paid 50 online fashion “influencers” to post Instagram pictures of themselves wearing the same paisley dress from the new collection, but failed to disclose they had given each influencer the dress, as well as thousands of dollars, in exchange for their endorsement.

In settling the charges, Lord & Taylor is prohibited from misrepresenting that paid ads are from an independent source, and is required to ensure that its influencers clearly disclose when they have been compensated in exchange for their endorsements.

“Lord & Taylor needs to be straight with consumers in its online marketing campaigns,” said Jessica Rich, Director of the FTC’s Bureau of Consumer Protection. “Consumers have the right to know when they’re looking at paid advertising.”

Design Lab Paisley Asymmetrical Dress that was the subject of the Nylon social media campaign

According to the FTC, over a weekend in late March 2015, Lord & Taylor launched a comprehensive social media campaign to promote its new Design Lab collection, a private-label clothing line targeted to women between 18 and 35 years old. The marketing plan included branded blog posts, photos, video uploads, native advertising editorials in online fashion magazines, and online endorsements by a team of specially selected “fashion influencers.”

The complaint alleges that Lord & Taylor placed a Lord & Taylor-edited paid article in *Nylon*, a pop culture and fashion publication. *Nylon* also posted a photo of the retailer’s Design Lab Paisley Asymmetrical Dress on *Nylon*’s Instagram site, along with a caption that Lord & Taylor had reviewed and approved. The Instagram post and article gave no indication to consumers that they were paid advertising placed by Lord & Taylor.

Over the same weekend in March 2015, Lord & Taylor gave 50 select fashion influencers a free Paisley Asymmetrical Dress and paid them between \$1,000 and \$4,000 each to post [a photo of themselves wearing it on Instagram or another social media site](#). While the influencers could style the dress any way they chose, Lord & Taylor contractually obligated them to use the “@lordandtaylor” Instagram user designation and the hashtag “#DesignLab” in the caption of the photo they posted. The company also pre-approved each proposed post.

In addition, the FTC’s complaint charges that Lord & Taylor did not require the influencers to disclose that the company had compensated them to post the photo, and none of the posts included such a disclosure. In total, the influencers’ posts reached 11.4 million individual Instagram users over just two days, led to 328,000 brand engagements with Lord & Taylor’s own Instagram handle, and the dress quickly sold out.

The proposed consent order settling the FTC’s complaint prohibits Lord & Taylor from misrepresenting that paid commercial advertising is from an independent or objective source. It also prohibits the company from misrepresenting that any endorser is an independent or ordinary consumer, and requires the company to disclose any unexpected material connection between itself and any influencer or endorser. Finally, it establishes a monitoring and review program for the company’s endorsement campaigns.

The FTC recently issued an [enforcement policy statement](#) that businesses can use to ensure they make required disclosures in native advertisements.

The Commission vote to issue the administrative complaint and to accept the proposed consent agreement was 4-0. The FTC will publish a description of the consent agreement package in the Federal Register shortly.

The agreement will be subject to public comment for 30 days, beginning today and continuing through April 14, 2016, after which the Commission will decide whether to make the proposed consent order final. Interested parties can [submit comments electronically](#) by following the instructions in the “Invitation To Comment” part of the “Supplementary Information” section.

NOTE: The Commission issues an administrative complaint when it has “reason to believe” that the law has been or is being violated, and it appears to the Commission that a proceeding is in the public interest. When the Commission issues a consent order on a final basis, it carries the force of law with respect to future actions. Each violation of such an order may result in a civil penalty of up to \$16,000.

<https://www.ftc.gov/news-events/press-releases/2016/03/lord-taylor-settles-ftc-charges-it-deceived-consumers-through>

5. Lord & Taylor gifted the Paisley Asymmetrical Dress to 50 select fashion influencers who were paid, in amounts ranging from \$1,000 to \$4,000, to post on the social media platform Instagram one photo of themselves wearing the Design Lab dress during a specified timeframe during the weekend of March 27-28, 2015. While the influencers were given the freedom to style the dress in any way they saw fit, Lord & Taylor contractually obligated them to exclusively mention the company using the “@lordandtaylor” Instagram user designation and the campaign hashtag “#DesignLab” in the photo caption. The influencers also were required to tag their photos of the dress using the “@lordandtaylor” Instagram designation.
6. Although Lord & Taylor’s Design Lab influencer contracts detailed the manner in which Respondent was to be mentioned in each Instagram posting, the contracts did not require the influencers to disclose in their postings that Respondent had compensated them, nor did Respondent otherwise obligate the influencers to disclose that they had been compensated.
7. In advance of the March 27-28, 2015 Design Lab debut, Respondent’s representatives pre-approved each of the influencers’ Instagram posts to ensure that the required campaign hashtag and the @lordandtaylor Instagram user designation were included in the photo captions. Respondent also made certain other stylistic edits to the influencers’ proposed text. None of the Instagram posts presented to Respondent for pre-approval included a disclosure that the influencer had received the dress for free, that she had been compensated for the post, or that the post was a part of a Lord & Taylor advertising campaign. Respondent Lord & Taylor did not edit any of the 50 posts to add such disclosures. *See Exhibit A* (representative Design Lab Instagram posts from the weekend of March 27-28, 2015).
8. The Design Lab Instagram campaign reached 11.4 million individual Instagram users, resulted in 328,000 brand engagements with Lord & Taylor’s own Instagram user handle (such as likes, comments, or re-postings), and the dress subsequently sold out.
9. Respondent’s Design Lab debut also included strategic placement of Lord & Taylor-edited Instagram posts and an article in online fashion magazines. One such magazine was Nylon, a pop culture and fashion publication owned by Nylon Media, LLC, the company that represented the majority of the fashion influencers involved in Respondent’s Design Lab Instagram campaign. Nylon posted a photo of the Paisley Asymmetrical Dress, along with a Lord & Taylor-edited caption, on its Instagram account during the product bomb weekend. *See Exhibit B* (Nylon.com Design Lab Instagram Post). Although paid for, reviewed, and pre-approved by Lord & Taylor, Nylon’s Instagram post failed to disclose that Lord & Taylor had paid for the posting.
10. Nylon Magazine also ran an article about the Design Lab collection in its online magazine on March 31, 2015. Under the terms of its contract with Nylon Magazine, Lord & Taylor reviewed and pre-approved the paid-for Nylon Design Lab article, yet the article did not disclose or otherwise make clear this commercial arrangement. *See Exhibit C* (Nylon.com Design Lab magazine article).

COUNT I**Misrepresentations About the Design Lab Instagram Postings**

11. Through the means described in Paragraphs 4 through 7, Respondent represented, directly or indirectly, expressly or by implication, that the 50 Instagram images and captions reflected the independent statements of impartial fashion influencers.
12. In fact, the 50 Instagram images and captions did not reflect the independent statements of impartial fashion influencers. Respondent's influencers specifically created the postings as part of an advertising campaign to promote sales of Respondent's Design Lab collection. Therefore, the representation set forth in Paragraph 11 is false or misleading.

COUNT II**Failure to Disclose Influencers' Material Connection to Lord & Taylor**

13. Through the means described in Paragraphs 4 through 7, Respondent represented, directly or indirectly, expressly or by implication, that the 50 Instagram images and captions posted on March 27 and 28, 2015 about the Paisley Asymmetrical Dress reflected the opinions of individuals with expertise in new trends in fashion. In numerous instances, Respondent failed to disclose or disclose adequately that these individuals were paid endorsers for Respondent. These facts would be material to consumers in their decision to purchase the Paisley Asymmetrical Dress. The failure to disclose these facts, in light of the representation made, was and is, a deceptive practice.

COUNT III**Misrepresentations About the Nylon Instagram Post
and the March 31, 2015 Nylon Magazine Article**

14. Through the means described in Paragraphs 9 and 10, Respondent represented, directly or indirectly, expressly or by implication, that the article that appeared on the March 31, 2015 Nylon Magazine website and the Design Lab posting on Nylon's Instagram account, were independent statements and opinions regarding the launch of Respondent's Design Lab collection.
15. In fact, neither the Nylon Magazine article nor the Nylon Instagram post were independent statements or opinions regarding Respondent's Design Lab collection; they were paid commercial advertising. Therefore, the representation set forth in Paragraph 14 is false or misleading.
16. The acts and practices of Respondent as alleged in this complaint constitute unfair or deceptive acts or practices in or affecting commerce in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a).

THEREFORE, the Federal Trade Commission this twentieth day of May, 2016, has issued this Complaint against Respondent.

By the Commission.

Donald S. Clark
Secretary

SEAL:



wendyslookbook

Follow

3 weeks ago

{spring awakening} Pairing a cropped trench with @lordandtaylor's exclusive #DesignLab handkerchief-hem dress 🌸 Really enjoyed seeing how others styled this vibrant piece!

leslieesue, tenun_ruseni, princesse_malgres_elle and 12.3k others like this.



hafizahadee

I want that shoesss []



thatsotee

AWESOME ☆



wendysundari

@chloe_little_store



nafiskerondotcom

@wendyslookbook it was such a pleasure to meet you today Wendy your a pure gem [] lets stay connected .



fashioninfinity12_

I post many ootds and designer handbags pics []



sabine_says

It's not that exclusive. I have seen about a dozen people style this on Instagram and many more when I looked at the hash tag...



Leave a comment...





caraasantana

Follow

3 weeks ago - 📍 CaraDisclothed.com
 Printed Paisley Perfection // Featuring @LordAndTaylor
 // New #DesignLab Collection //

♥️ **jhonsbdjld, laszx4, extracc** and 1,498 others like this.



chrissiebixler
 You are such a pretty girl. 📷



lillimaumus
 Beautiful dress !



princeslola2015
 body goals



jennee115
 @kaye_yuki lol same dress



Leave a comment...





feralcreature

Follow

3 weeks ago

Spring in my step and on my body. Getting festival-ready is a piece of cake with this dress thanks to @lordandtaylor and their new #DesignLab collection. Holla at me, Coachella.

♡ **jorge_sclar, muhaymenulislam, edyedy.t** and 7,602 others like this.



feralcreature
#lordandtaylor



abigailx56
Beautiful c



ukvintageflorence
🇬🇧英国🇬🇧vintage🇬🇧jewelry🇬🇧首饰控follow my wechat!



yeshidl
Woww



monpipit
You're so good looking @feralcreature



zanepeck



ksdnyc
@aweks315 ♥♥♥♥♥♥♥♥♥♥



nanauban70

♡ Leave a comment... ⋮



happilygrey 3 weeks ago Follow

Earlier this week enjoying the warmer temps and @lordandtaylor new #DesignLab collection feat. this breezy handkerchief dress #summerready #boho

emis_killa_fanpage_click_in, myfashionmission, scraps.of.style and 3,177 others like this.

traveljunkiediary @larataki who wore it best? 🌍

brokegirlstyle 🌈🌈🌈

cherie.chloe In♥with shoes!

black_instinct New fashion account 🌹

iwanek_00 Love ♥

sidewalkstyleblog Literally love all your outfits!

larataki @traveljunkiediary 🌍

rouxclues 🌍

Leave a comment...



sidesmilestyle

Follow

4 weeks ago · www.sidesmilestyle.com
 dancing in #designlab today on the blog | shop my exact look here (dress is only \$88!) --> @liketoknow.it
www.liketk.it/19nLg #liketkit #dallasblogger #LTshop

♥ koko232332, rwaiah2_3333, thaqibimran and 421 others like this.



simplyduostyle

So cute!



anextraordinaryaffaire

So nice to "meet" a fellow blogger in Dallas! Enjoy your day! Love your style! @sidesmilestyle 📷



paxandparker

Loving that green door!



alittlecasual

Gorgeous dress!! 🍷



Leave a comment...





N nylonmag

4 weeks ago

Our editor-in-chief @heymichellelee transitioned her everyday outfit into the perfect springtime ensemble with this patterned dress by @lordandtaylor's new #DesignLab collection 📷

Follow

♥ valeria_santizo, arianatorforever100, miriam_gurdian2004 and 4,027 others like this.



sarita10612

@emitre17



la_vie_boheme85

@kndnyc Did they raid your closet?



likecandey

who makes the jacket?



conte_eleni_

@annamaria.banakou



leanweezy

@relol



lagirlygirl

@hawamoj on fleek



hawamoj

@lagirlygirl for outside land



leslie1981



Leave a comment...



NYLON



FASHION

BEAUTY

RADAR

MUSIC

THE MAGAZINE

SHOP

SUBSCRIBE

VIDEO

ESPAÑOL

GUYS



film

stop what you're doing and watch the new 'mad max' trailer

seriously, stop.



fashion

this season's must-have line

lord & taylor's design lab



radar



music

subscribe

giveagift



advertise

newsletter

#NYLON shop



FROM OUR FASHION CLOSET TO YOURS

SHOP NOW >>



this season's must-have line

lord & taylor's design lab

by: nylon — march 31 2015

#NYLONshop

FROM OUR FASHION CLOSET TO YOURS

SHOP NOW >>



more nylon

prev **rihanna** finally speaks out about dating **leonardo dicaprio**



next **stop what you're doing and watch the new 'mad max' trailer**



from our friends



Bobbi Kristina Brown



9 Must-Know Tips For



view gallery

photo via @alwaysjudging instagram



Every season, there's one collection that you see everywhere—and yet, instead of getting sick of it, you lust after it until one day, you finally cave in and get it for yourself. This time around, we're taking out the guess work and introducing you to spring's must-have line: **Lord & Taylor's Design Lab**. You've probably already seen the new contemporary line's asymmetric bandana dress everywhere—from Instagram to your favorite blogs to the streets. But **Design Lab** is filled with many more amazing statement pieces, like festival-ready lazer cut tanks and fringed kimonos.

Click through the gallery to see how your favorite bloggers style their **Design Lab** pieces.

withdraw its acceptance of this agreement and so notify Proposed Respondent, in which event it will take such action as it may consider appropriate, or issue and serve its complaint (in such form as the circumstances may require) and decision in disposition of the proceeding.

4. Proposed Respondent neither admits nor denies any of the allegations in the draft complaint, except as specifically stated in this order. Only for purposes of this action, Proposed Respondent admits the facts necessary to establish jurisdiction.

5. This agreement contemplates that, if it is accepted by the Commission, and if such acceptance is not subsequently withdrawn by the Commission pursuant to the provisions of Section 2.34 of the Commission's Rules, the Commission may, without further notice to Proposed Respondent, (1) issue its complaint corresponding in form and substance with the attached draft complaint and its decision containing the following order in disposition of the proceeding, and (2) make information about it public. When so entered, the order shall have the same force and effect and may be altered, modified, or set aside in the same manner and within the same time frame provided by statute for other orders. The order shall become final upon service. Delivery of the complaint and the decision and order to Proposed Respondent's address as stated in this agreement by any means specified in Section 4.4(a) of the Commission's Rules shall constitute service. Proposed Respondent waives any right it may have to any other manner of service. The complaint may be used in construing the terms of the order, and no agreement, understanding, representation, or interpretation not contained in the order or the agreement may be used to vary or contradict the terms of the order.

6. Proposed Respondent has read the draft complaint and consent order. Proposed Respondent understands that it may be liable for civil penalties in the amount provided by law and other appropriate relief for each violation of the order after it becomes final.

ORDER

DEFINITIONS

For purposes of this order, the following definitions shall apply:

1. Unless otherwise specified, "Respondent" shall mean Lord & Taylor, LLC, a limited liability company, its successors and assigns, and its officers, agents, representatives, and employees.
2. "Clear(ly) and conspicuous(ly)" means that a required disclosure is difficult to miss (*i.e.*, easily noticeable) and easily understandable by ordinary consumers, including in all of the following ways:
 - a. In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the communication is presented. In any communication made through both visual and audible means, the disclosure must be presented simultaneously in both the visual and audible portions of the

- communication even if the representation requiring the disclosure is made in only one means.
- b. A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.
 - c. An audible disclosure, including by streaming video, must be delivered in a volume, speed, and cadence sufficient for ordinary consumers to easily hear and understand it.
 - d. In any communication using an interactive electronic medium, such as the Internet or software, the disclosure must be unavoidable.
 - e. The disclosure must use diction and syntax understandable to ordinary consumers and must appear in each language in which the representation that requires the disclosure appears.
 - f. The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices.
 - g. The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.
 - h. When the representation or sales practice targets a specific audience, such as children, the elderly, or the terminally ill, “ordinary consumers” includes reasonable members of that group.
3. “Close proximity” means that the disclosure is very near the triggering endorsement or representation. In an interactive electronic medium (such as a mobile app or other computer program), a visual disclosure that cannot be viewed at the same time and in the same viewable area as the triggering endorsement or representation, on the technology used by ordinary consumers, is not in close proximity. A disclosure made through a hyperlink, pop-up, interstitial, or other similar technique is not in close proximity to the triggering endorsement or representation. A disclosure made on a different printed page than the triggering endorsement or representation is not in close proximity.
4. “Commerce” means as defined in Section 4 of the Federal Trade Commission Act, 15 U.S.C. § 44.
5. “Endorsement” means any advertising message (including verbal statements, demonstrations, or depictions of the name, signature, likeness, or other identifying personal characteristics of an individual or the name or seal of an organization) that consumers are likely to believe reflects the opinions, beliefs, findings, or experiences of a party other than the sponsoring advertiser, even if the views expressed by that party are identical to those of the sponsoring advertiser.

6. “Endorser” means an individual or organization that provides an endorsement.
7. “Influencer Campaign” means any arrangement whereby, in connection with the advertising, promotion, offering for sale, sale, or distribution of any product or service, Respondent engages an endorser (also known as an Influencer) to create, publish, or otherwise disseminate an endorsement and the endorser has a material connection to Respondent, or any other person or entity acting on Respondent’s behalf.
8. “Material connection” means any relationship that materially affects the weight or credibility of any endorsement and that would not be reasonably expected by consumers.

I.

IT IS ORDERED that Respondent, directly or through any corporation, partnership, subsidiary, division, or other device, in connection with the advertising, labeling, promotion, offering for sale, sale, or distribution of any product or service, in or affecting commerce, shall not misrepresent, in any manner, expressly or by implication, that an endorser of such product or service is an independent user or ordinary consumer of the product or service.

II.

IT IS FURTHER ORDERED that Respondent, directly or through any corporation, partnership, subsidiary, division, or other device, in connection with the advertising, labeling, promotion, offering for sale, sale, or distribution of any product or service, in or affecting commerce, by means of an endorsement of such product or service, shall clearly and conspicuously, and in close proximity to the representation, disclose a material connection, if one exists, between such endorser and Respondent.

III.

IT IS FURTHER ORDERED that Respondent, and its successors and assigns, shall not misrepresent, in any manner, expressly or by implication, that paid commercial advertising is a statement or opinion from an independent or objective publisher or source.

IV.

IT IS FURTHER ORDERED that Respondent, directly or through any corporation, partnership, subsidiary, division, or other device, in connection with the advertising, labeling, promotion, offering for sale, sale, or distribution of any product or service, in or affecting commerce, by means of an endorsement by an endorser with a material connection to Respondent, shall take steps sufficient to ensure compliance with Parts I and II of this order. Such steps shall include, at a minimum:

- A. Providing each such endorser with a clear statement of his or her responsibility to disclose, clearly and conspicuously, in any print, radio, television, online, or digital

advertisement or communication, including but not limited to Instagram or blog posts, the endorser's material connection to Respondent, and obtaining from each such endorser a signed and dated statement acknowledging receipt of that statement and expressly agreeing to comply with it;

- B. Establishing, implementing, and thereafter maintaining a system to monitor and review the representations and disclosures of endorsers, made as part of an Influencer Campaign, with material connections to Respondent to ensure compliance with Parts I and II of this order. The system shall include, at a minimum, monitoring and reviewing its endorsers' print, radio, television, online, or digital advertisements or communications made as part of an Influencer Campaign;
- C. Immediately terminating any endorser with a material connection to Respondent who Respondent reasonably concludes:
 - 1. Has misrepresented, in any manner, his or her independence and impartiality; or
 - 2. Has failed to disclose, clearly and conspicuously, and in close proximity to the representation, a material connection between such endorser and Respondent;

Provided, however, that Respondent may provide an endorser with one notice of a failure to disclose and an opportunity to cure the disclosure prior to terminating the endorser if Respondent reasonably concludes that the failure to disclose was inadvertent; Respondent shall inform any endorser to whom it has provided a notice of a failure to disclose a material connection that any subsequent failure to disclose will result in immediate termination; and

- D. Creating, and thereafter maintaining, reports sufficient to show the results of the monitoring required by subpart B of this Part of the order.

V.

IT IS FURTHER ORDERED that Respondent, and its successors and assigns, shall, for five (5) years after the last date of dissemination of any representation or endorsement covered by this order, maintain and upon reasonable notice make available to the Federal Trade Commission for inspection and copying:

- A. All advertisements and promotional materials containing the representation or endorsement;
- B. All contracts and written communications concerning or relating to the disclosures required by Part II of this order with any endorser engaged by Respondent, or any other person or entity acting on Respondent's behalf, to participate in any Influencer Campaign;

- C. Any documents that comprise or relate to complaints or inquiries related to the subject matter of this order, whether received directly, indirectly, or through any third party, that concern any endorsement made or disseminated by Respondent, or on behalf of Respondent, and any responses to those complaints or inquiries;
- D. Any documents reasonably necessary to demonstrate full compliance with each provision of this order, including but not limited to, all documents obtained, created, generated, or which in any way relate to the requirements, provisions, terms of this order, and all reports submitted to the Commission pursuant to this order;
- E. Any documents that contradict, qualify, or call into question Respondent's compliance with this order; and
- F. All acknowledgments of receipt of this order obtained pursuant to Part VI.

VI.

IT IS FURTHER ORDERED that Respondent, and its successors and assigns, shall deliver a copy of this order to all current and future principals, officers, and directors, and to all current and future managers, employees, agents, and representatives having responsibilities with respect to the subject matter of this order, and shall secure from each person a signed and dated statement acknowledging receipt of this order. Respondent shall deliver this order to such current personnel within thirty (30) days after the date of service of this order and to future personnel within thirty (30) days after the person assumes such position or responsibilities.

VII.

IT IS FURTHER ORDERED that Respondent, and its successors and assigns, shall notify the Commission at least thirty (30) days prior to any change in the corporation that may affect compliance obligations arising under this order, including, but not limited to, dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor corporation; the creation or dissolution of a subsidiary, parent, or related entity that engages in any acts or practices subject to this order; the proposed filing of a bankruptcy petition; or a change in the corporate name or address. Provided, however, that, with respect to any proposed change in the corporation about which Respondent learns less than thirty (30) days prior to the date such action is to take place, Respondent shall notify the Commission as soon as is practicable after obtaining such knowledge. Unless otherwise directed by a representative of the Commission in writing, these reports shall be emailed to Debrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580. The subject line must begin: *In re Lord & Taylor*.

VIII.

IT IS FURTHER ORDERED that Respondent, and its successors and assigns, within ninety (90) days after the date of service of this order, shall file with the Commission a true and accurate report, in writing, setting forth in detail the manner and form of its compliance with this order. Within ten (10) days of receipt of written notice from a representative of the Commission, it shall submit additional true and accurate written reports. Unless otherwise directed by a representative of the Commission in writing, these reports shall be emailed to Debrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580. The subject line must begin: *In re Lord & Taylor*.

IX.

This order will terminate twenty (20) years from the date of its issuance, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint (with or without an accompanying consent decree) in federal court alleging any violation of the order, whichever comes later; provided, however, that the filing of such a complaint will not affect the duration of:

- A. Any Part in this order that terminates in less than twenty (20) years; and
- B. This order if such complaint is filed after the order has terminated pursuant to this Part.

Provided, further, that if such complaint is dismissed or a federal court rules that Respondent did not violate any provision of the order, and the dismissal or ruling is either not appealed or upheld on appeal, then the order will terminate according to this Part as though the complaint had never been filed, except that the order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

Lord & Taylor, LLC

Date: _____

 Elizabeth Rodbell
 President
 Hudson's Bay Company DSG

Date: _____

 David G. Mallen

Nathan J. Muyskens
Loeb & Loeb LLP
Counsel for Lord & Taylor

Date: _____

Robin Rosen Spector
Counsel for the Federal Trade Commission

APPROVED:

MARY K. ENGLE
Associate Director
Division of Advertising Practices

JESSICA L. RICH
Director
Bureau of Consumer Protection

NOW, CRACK THE CODE
TO YOUNGER ACTING SKIN.

NEW
YOUTH CODE™
Youth Regenerating Skincare

ONE DROP
INSTANTLY IMPROVES SKIN QUALITY

ONE WEEK
SKIN BEGINS TO LOOK YOUNGER

ONE MONTH
REVEAL THE NEW YOUTH OF YOUR SKIN**

10 YEARS OF GENE RESEARCH
INTERNATIONAL PATENT

Because you're worth it™
L'ORÉAL
PARIS

THE NEW ERA OF SKINCARE:
GENE SCIENCE.

Imagine... what if you could grow young?
Every great discovery begins by pushing
the boundaries of science. After 10 years
of research, now we know that recovery
genes in youthful skin respond 5x faster
to aggressions than aging skin does. So
even though you can't grow young, we
now have the knowledge to help you begin
cracking the code to younger acting skin.

CLINICAL STUDY:
5X FASTER

GENE RESPONSE TO AGGRESSIONS
AGING SKIN YOUTHFUL SKIN

A dramatic new possibility against
the signs of aging:
L'Oréal introduces Youth Regenerating
Skincare. New Youth Code Serum Intense
with GenActiv Technology™. Designed to
help increase skin's ability to recover faster
from aggressions more like it did when it
was younger.* With Youth Code, now you can
instantly improve skin quality while revealing
the new youth of your skin**

Discover all of the Youth Code products
and learn more about gene science.
L'ORÉAL.PARIS.COM/YOUTHCODE

*Based on in vivo testing. **Skin is more youthful looking.
©2011 L'Oréal USA, Inc.

L'Oréal Settles FTC Charges Alleging Deceptive Advertising for Anti-Aging Cosmetics

Claims that Skincare Products Targeted Users' Genes Were Misleading, FTC Says

Cosmetics company L'Oréal USA, Inc. has agreed to [settle Federal Trade Commission charges of deceptive advertising](#) about its Lancôme Génifique and L'Oréal Paris Youth Code skincare products. According to the FTC's complaint, L'Oréal made false and unsubstantiated claims that its Génifique and Youth Code products provided anti-aging benefits by targeting users' genes.

"It would be nice if cosmetics could alter our genes and turn back time," said Jessica Rich, Director of the FTC's Bureau of Consumer Protection. "But L'Oréal couldn't support these claims."

In national advertising campaigns that encompassed print, radio, television, Internet, and social media outlets, L'Oréal claimed that its Génifique products were “clinically proven” to “[boost genes' activity and stimulate the production of youth proteins](#)” that would cause “visibly younger skin in just 7 days,” and would provide results to specific percentages of users.

Portion of L'oreal Youth Code print advertisement. (click to view full ad)

Similarly, for its Youth Code products, L'Oréal touted – in both English- and Spanish-language advertisements – the “new era of skincare: gene science,” and that consumers could “[crack the code to younger acting skin](#).”

Charging as much as \$132 per container, L'Oréal has sold Génifique nationwide since February 2009 at Lancôme counters in department stores and at beauty specialty stores. The company has sold Youth Code, which costs up to \$25 per container at major retail stores across the United States, since November 2010.

Under the [proposed administrative settlement](#), L'Oréal is prohibited from claiming that any Lancôme brand or L'Oréal Paris brand facial skincare product targets or boosts the activity of genes to make skin look or act younger, or respond five times faster to aggressors like stress, fatigue, and aging, unless the company has competent and reliable scientific evidence substantiating such claims. The settlement also prohibits claims that certain Lancôme brand and L'Oréal Paris brand products affect genes unless the claims are supported by competent and reliable scientific evidence. Finally, L'Oréal is prohibited from making claims about these products that misrepresent the results of any test or study.

The Commission vote to accept the consent agreement package containing the proposed consent order for public comment was 4-0-1, with Commissioner McSweeney not participating.

The FTC will publish a description of the consent agreement in the Federal Register shortly. The agreement will be subject to public comment for 30 days, beginning today and continuing through July 30, 2014, after which the Commission will decide whether to make the proposed consent order final. Interested parties can submit written comments electronically or in paper form by following the instructions in “Supplementary Information” section of the Federal Register notice. Comments should be submitted electronically using the form [at this link](#). Instructions for submitting comments in paper form are listed in the “Accessibility” portion of the form.

NOTE: The Commission issues an administrative complaint when it has “reason to believe” that the law has been or is being violated, and it appears to the Commission that a proceeding is in the public interest. When the Commission issues a consent order on a final basis, it carries the force of law with respect to future actions. Each violation of such an order may result in a civil penalty of up to \$16,000.

FEDERAL TRADE COMMISSION
16 CFR Part 255

Guides Concerning the Use of Endorsements and Testimonials in Advertising

* * * *

This document includes only the text of the Revised Endorsement and Testimonial Guides. To learn more, read the Federal Register Notice at www.ftc.gov/opa/2009/10/endortest.shtm.

* * * *

§ 255.0 Purpose and definitions.

(a) The Guides in this part represent administrative interpretations of laws enforced by the Federal Trade Commission for the guidance of the public in conducting its affairs in conformity with legal requirements. Specifically, the Guides address the application of Section 5 of the FTC Act (15 U.S.C. 45) to the use of endorsements and testimonials in advertising. The Guides provide the basis for voluntary compliance with the law by advertisers and endorsers. Practices inconsistent with these Guides may result in corrective action by the Commission under Section 5 if, after investigation, the Commission has reason to believe that the practices fall within the scope of conduct declared unlawful by the statute.

The Guides set forth the general principles that the Commission will use in evaluating endorsements and testimonials, together with examples illustrating the application of those principles. The Guides do not purport to cover every possible use of endorsements in advertising. Whether a particular endorsement or testimonial is deceptive will depend on the specific factual circumstances of the advertisement at issue.

(b) For purposes of this part, an endorsement means any advertising message (including verbal statements, demonstrations, or depictions of the name, signature, likeness or other identifying personal characteristics of an individual or the name or seal of an organization) that consumers are likely to believe reflects the opinions, beliefs, findings, or experiences of a party other than the sponsoring advertiser, even if the views expressed by that party are identical to those of the sponsoring advertiser. The party whose opinions, beliefs, findings, or experience the message appears to reflect will be called the endorser and may be an individual, group, or institution.

(c) The Commission intends to treat endorsements and testimonials identically in the context of its enforcement of the Federal Trade Commission Act and for purposes of this part. The term endorsements is therefore generally used hereinafter to cover both terms and situations.

(d) For purposes of this part, the term product includes any product, service, company or industry.

(e) For purposes of this part, an expert is an individual, group, or institution possessing, as a result of experience, study, or training, knowledge of a particular subject, which knowledge is superior to what ordinary individuals generally acquire.

Example 1: A film critic's review of a movie is excerpted in an advertisement. When so used, the review meets the definition of an endorsement because it is viewed by readers as a statement of the critic's own opinions and not those of the film producer, distributor, or exhibitor. Any alteration in or quotation from the text of the review that does not fairly reflect its substance would be a violation of the standards set by this part because it would distort the endorser's opinion. [See § 255.1(b).]

Example 2: A TV commercial depicts two women in a supermarket buying a laundry detergent. The women are not identified outside the context of the advertisement. One comments to the other how clean her brand makes her family's clothes, and the other then comments that she will try it because she has not been fully satisfied with her own brand. This obvious fictional dramatization of a real life situation would not be an endorsement.

Example 3: In an advertisement for a pain remedy, an announcer who is not familiar to consumers except as a spokesman for the advertising drug company praises the drug's ability to deliver fast and lasting pain relief. He purports to speak, not on the basis of his own opinions, but rather in the place of and on behalf of the drug company. The announcer's statements would not be considered an endorsement.

Example 4: A manufacturer of automobile tires hires a well-known professional automobile racing driver to deliver its advertising message in television commercials. In these commercials, the driver speaks of the smooth ride, strength, and long life of the tires. Even though the message is not expressly declared to be the personal opinion of the driver, it may nevertheless constitute an endorsement of the tires. Many consumers will recognize this individual as being primarily a racing driver and not merely a spokesperson or announcer for the advertiser. Accordingly, they may well believe the driver would not speak for an automotive product unless he actually believed in what he was saying and had personal knowledge sufficient to form that belief. Hence, they would think that the advertising message reflects the driver's personal views. This attribution of the underlying views to the driver brings the advertisement within the definition of an endorsement for purposes of this part.

Example 5: A television advertisement for a particular brand of golf balls shows a prominent and well-recognized professional golfer practicing numerous drives off the tee. This would be an endorsement by the golfer even though she makes no verbal statement in the advertisement.

Example 6: An infomercial for a home fitness system is hosted by a well-known entertainer. During the infomercial, the entertainer demonstrates the machine and states that it is the most effective and easy-to-use home exercise machine that she has ever tried. Even if she is reading from a script, this statement would be an endorsement, because consumers are likely to believe it reflects the entertainer's views.

Example 7: A television advertisement for a housewares store features a well-known female comedian and a well-known male baseball player engaging in light-hearted banter about products each one intends to purchase for the other. The comedian says that she will buy him a Brand X, portable, high-definition television so he can finally see the strike zone. He says that he will get her a Brand Y juicer so she can make juice with all the fruit

and vegetables thrown at her during her performances. The comedian and baseball player are not likely to be deemed endorsers because consumers will likely realize that the individuals are not expressing their own views.

Example 8: A consumer who regularly purchases a particular brand of dog food decides one day to purchase a new, more expensive brand made by the same manufacturer. She writes in her personal blog that the change in diet has made her dog's fur noticeably softer and shinier, and that in her opinion, the new food definitely is worth the extra money. This posting would not be deemed an endorsement under the Guides.

Assume that rather than purchase the dog food with her own money, the consumer gets it for free because the store routinely tracks her purchases and its computer has generated a coupon for a free trial bag of this new brand. Again, her posting would not be deemed an endorsement under the Guides.

Assume now that the consumer joins a network marketing program under which she periodically receives various products about which she can write reviews if she wants to do so. If she receives a free bag of the new dog food through this program, her positive review would be considered an endorsement under the Guides.

§ 255.1 General considerations.

(a) Endorsements must reflect the honest opinions, findings, beliefs, or experience of the endorser. Furthermore, an endorsement may not convey any express or implied representation that would be deceptive if made directly by the advertiser. [See §§ 255.2(a) and (b) regarding substantiation of representations conveyed by consumer endorsements.]

(b) The endorsement message need not be phrased in the exact words of the endorser, unless the advertisement affirmatively so represents. However, the endorsement may not be presented out of context or reworded so as to distort in any way the endorser's opinion or experience with the product. An advertiser may use an endorsement of an expert or celebrity only so long as it has good reason to believe that the endorser continues to subscribe to the views presented. An advertiser may satisfy this obligation by securing the endorser's views at reasonable intervals where reasonableness will be determined by such factors as new information on the performance or effectiveness of the product, a material alteration in the product, changes in the performance of competitors' products, and the advertiser's contract commitments.

(c) When the advertisement represents that the endorser uses the endorsed product, the endorser must have been a bona fide user of it at the time the endorsement was given. Additionally, the advertiser may continue to run the advertisement only so long as it has good reason to believe that the endorser remains a bona fide user of the product. [See § 255.1(b) regarding the "good reason to believe" requirement.]

(d) Advertisers are subject to liability for false or unsubstantiated statements made through endorsements, or for failing to disclose material connections between themselves and their endorsers [see § 255.5]. Endorsers also may be liable for statements made in the course of their endorsements.

Example 1: A building contractor states in an advertisement that he uses the advertiser's exterior house paint because of its remarkable quick drying properties and durability. This endorsement must comply with the pertinent requirements of Section 255.3 (Expert Endorsements). Subsequently, the advertiser reformulates its paint to enable it to cover exterior surfaces with only one coat. Prior to continued use of the contractor's endorsement, the advertiser must contact the contractor in order to determine whether the contractor would continue to specify the paint and to subscribe to the views presented previously.

Example 2: A television advertisement portrays a woman seated at a desk on which rest five unmarked computer keyboards. An announcer says, "We asked X, an administrative assistant for over ten years, to try these five unmarked keyboards and tell us which one she liked best." The advertisement portrays X typing on each keyboard and then picking the advertiser's brand. The announcer asks her why, and X gives her reasons. This endorsement would probably not represent that X actually uses the advertiser's keyboard at work. In addition, the endorsement also may be required to meet the standards of Section 255.3 (expert endorsements).

Example 3: An ad for an acne treatment features a dermatologist who claims that the product is "clinically proven" to work. Before giving the endorsement, she received a write-up of the clinical study in question, which indicates flaws in the design and conduct of the study that are so serious that they preclude any conclusions about the efficacy of the product. The dermatologist is subject to liability for the false statements she made in the advertisement. The advertiser is also liable for misrepresentations made through the endorsement. [See Section 255.3 regarding the product evaluation that an expert endorser must conduct.]

Example 4: A well-known celebrity appears in an infomercial for an oven roasting bag that purportedly cooks every chicken perfectly in thirty minutes. During the shooting of the infomercial, the celebrity watches five attempts to cook chickens using the bag. In each attempt, the chicken is undercooked after thirty minutes and requires sixty minutes of cooking time. In the commercial, the celebrity places an uncooked chicken in the oven roasting bag and places the bag in one oven. He then takes a chicken roasting bag from a second oven, removes from the bag what appears to be a perfectly cooked chicken, tastes the chicken, and says that if you want perfect chicken every time, in just thirty minutes, this is the product you need. A significant percentage of consumers are likely to believe the celebrity's statements represent his own views even though he is reading from a script. The celebrity is subject to liability for his statement about the product. The advertiser is also liable for misrepresentations made through the endorsement.

Example 5: A skin care products advertiser participates in a blog advertising service. The service matches up advertisers with bloggers who will promote the advertiser's products on their personal blogs. The advertiser requests that a blogger try a new body lotion and write a review of the product on her blog. Although the advertiser does not make any specific claims about the lotion's ability to cure skin conditions and the blogger does not ask the advertiser whether there is substantiation for the claim, in her review the blogger writes that the lotion cures eczema and recommends the product to her blog readers who suffer from this condition. The advertiser is subject to liability for misleading or unsubstantiated

representations made through the blogger's endorsement. The blogger also is subject to liability for misleading or unsubstantiated representations made in the course of her endorsement. The blogger is also liable if she fails to disclose clearly and conspicuously that she is being paid for her services. [See § 255.5.]

In order to limit its potential liability, the advertiser should ensure that the advertising service provides guidance and training to its bloggers concerning the need to ensure that statements they make are truthful and substantiated. The advertiser should also monitor bloggers who are being paid to promote its products and take steps necessary to halt the continued publication of deceptive representations when they are discovered.

§ 255.2 Consumer endorsements.

(a) An advertisement employing endorsements by one or more consumers about the performance of an advertised product or service will be interpreted as representing that the product or service is effective for the purpose depicted in the advertisement. Therefore, the advertiser must possess and rely upon adequate substantiation, including, when appropriate, competent and reliable scientific evidence, to support such claims made through endorsements in the same manner the advertiser would be required to do if it had made the representation directly, *i.e.*, without using endorsements. Consumer endorsements themselves are not competent and reliable scientific evidence.

(b) An advertisement containing an endorsement relating the experience of one or more consumers on a central or key attribute of the product or service also will likely be interpreted as representing that the endorser's experience is representative of what consumers will generally achieve with the advertised product or service in actual, albeit variable, conditions of use. Therefore, an advertiser should possess and rely upon adequate substantiation for this representation. If the advertiser does not have substantiation that the endorser's experience is representative of what consumers will generally achieve, the advertisement should clearly and conspicuously disclose the generally expected performance in the depicted circumstances, and the advertiser must possess and rely on adequate substantiation for that representation.¹

¹ The Commission tested the communication of advertisements containing testimonials that clearly and prominently disclosed either "Results not typical" or the stronger "These testimonials are based on the experiences of a few people and you are not likely to have similar results." Neither disclosure adequately reduced the communication that the experiences depicted are generally representative. Based upon this research, the Commission believes that similar disclaimers regarding the limited applicability of an endorser's experience to what consumers may generally expect to achieve are unlikely to be effective.

Nonetheless, the Commission cannot rule out the possibility that a strong disclaimer of typicality could be effective in the context of a particular advertisement. Although the Commission would have the burden of proof in a law enforcement action, the Commission notes that an advertiser possessing reliable empirical testing demonstrating that the net impression of its advertisement with such a disclaimer is non-deceptive will avoid the risk of the initiation of such an action in the first instance.

(c) Advertisements presenting endorsements by what are represented, directly or by implication, to be “actual consumers” should utilize actual consumers in both the audio and video, or clearly and conspicuously disclose that the persons in such advertisements are not actual consumers of the advertised product.

Example 1: A brochure for a baldness treatment consists entirely of testimonials from satisfied customers who say that after using the product, they had amazing hair growth and their hair is as thick and strong as it was when they were teenagers. The advertiser must have competent and reliable scientific evidence that its product is effective in producing new hair growth.

The ad will also likely communicate that the endorsers’ experiences are representative of what new users of the product can generally expect. Therefore, even if the advertiser includes a disclaimer such as, “Notice: These testimonials do not prove our product works. You should not expect to have similar results,” the ad is likely to be deceptive unless the advertiser has adequate substantiation that new users typically will experience results similar to those experienced by the testimonialists.

Example 2: An advertisement disseminated by a company that sells heat pumps presents endorsements from three individuals who state that after installing the company’s heat pump in their homes, their monthly utility bills went down by \$100, \$125, and \$150, respectively. The ad will likely be interpreted as conveying that such savings are representative of what consumers who buy the company’s heat pump can generally expect. The advertiser does not have substantiation for that representation because, in fact, less than 20% of purchasers will save \$100 or more. A disclosure such as, “Results not typical” or, “These testimonials are based on the experiences of a few people and you are not likely to have similar results” is insufficient to prevent this ad from being deceptive because consumers will still interpret the ad as conveying that the specified savings are representative of what consumers can generally expect. The ad is less likely to be deceptive if it clearly and conspicuously discloses the generally expected savings and the advertiser has adequate substantiation that homeowners can achieve those results. There are multiple ways that such a disclosure could be phrased, *e.g.*, “the average homeowner saves \$35 per month,” “the typical family saves \$50 per month during cold months and \$20 per month in warm months,” or “most families save 10% on their utility bills.”

Example 3: An advertisement for a cholesterol-lowering product features an individual who claims that his serum cholesterol went down by 120 points and does not mention having made any lifestyle changes. A well-conducted clinical study shows that the product reduces the cholesterol levels of individuals with elevated cholesterol by an average of 15% and the advertisement clearly and conspicuously discloses this fact. Despite the presence of this disclosure, the advertisement would be deceptive if the advertiser does not have adequate substantiation that the product can produce the specific results claimed by the endorser (*i.e.*, a 120-point drop in serum cholesterol without any lifestyle changes).

Example 4: An advertisement for a weight-loss product features a formerly obese woman. She says in the ad, “Every day, I drank 2 WeightAway shakes, ate only raw vegetables, and exercised vigorously for six hours at the gym. By the end of six months, I had gone from 250 pounds to 140 pounds.” The advertisement accurately describes the woman’s

experience, and such a result is within the range that would be generally experienced by an extremely overweight individual who consumed WeightAway shakes, only ate raw vegetables, and exercised as the endorser did. Because the endorser clearly describes the limited and truly exceptional circumstances under which she achieved her results, the ad is not likely to convey that consumers who weigh substantially less or use WeightAway under less extreme circumstances will lose 110 pounds in six months. (If the advertisement simply says that the endorser lost 110 pounds in six months using WeightAway together with diet and exercise, however, this description would not adequately alert consumers to the truly remarkable circumstances leading to her weight loss.) The advertiser must have substantiation, however, for any performance claims conveyed by the endorsement (*e.g.*, that WeightAway is an effective weight loss product).

If, in the alternative, the advertisement simply features “before” and “after” pictures of a woman who says “I lost 50 pounds in 6 months with WeightAway,” the ad is likely to convey that her experience is representative of what consumers will generally achieve. Therefore, if consumers cannot generally expect to achieve such results, the ad should clearly and conspicuously disclose what they can expect to lose in the depicted circumstances (*e.g.*, “most women who use WeightAway for six months lose at least 15 pounds”).

If the ad features the same pictures but the testimonialist simply says, “I lost 50 pounds with WeightAway,” and WeightAway users generally do not lose 50 pounds, the ad should disclose what results they do generally achieve (*e.g.*, “most women who use WeightAway lose 15 pounds”).

Example 5: An advertisement presents the results of a poll of consumers who have used the advertiser’s cake mixes as well as their own recipes. The results purport to show that the majority believed that their families could not tell the difference between the advertised mix and their own cakes baked from scratch. Many of the consumers are actually pictured in the advertisement along with relevant, quoted portions of their statements endorsing the product. This use of the results of a poll or survey of consumers represents that this is the typical result that ordinary consumers can expect from the advertiser’s cake mix.

Example 6: An advertisement purports to portray a “hidden camera” situation in a crowded cafeteria at breakfast time. A spokesperson for the advertiser asks a series of actual patrons of the cafeteria for their spontaneous, honest opinions of the advertiser’s recently introduced breakfast cereal. Even though the words “hidden camera” are not displayed on the screen, and even though none of the actual patrons is specifically identified during the advertisement, the net impression conveyed to consumers may well be that these are actual customers, and not actors. If actors have been employed, this fact should be clearly and conspicuously disclosed.

Example 7: An advertisement for a recently released motion picture shows three individuals coming out of a theater, each of whom gives a positive statement about the movie. These individuals are actual consumers expressing their personal views about the movie. The advertiser does not need to have substantiation that their views are representative of the opinions that most consumers will have about the movie. Because the consumers’ statements would be understood to be the subjective opinions of only three people, this advertisement is not likely to convey a typicality message.

If the motion picture studio had approached these individuals outside the theater and offered them free tickets if they would talk about the movie on camera afterwards, that arrangement should be clearly and conspicuously disclosed. [See § 255.5.]

§ 255.3 Expert endorsements.

(a) Whenever an advertisement represents, directly or by implication, that the endorser is an expert with respect to the endorsement message, then the endorser's qualifications must in fact give the endorser the expertise that he or she is represented as possessing with respect to the endorsement.

(b) Although the expert may, in endorsing a product, take into account factors not within his or her expertise (*e.g.*, matters of taste or price), the endorsement must be supported by an actual exercise of that expertise in evaluating product features or characteristics with respect to which he or she is expert and which are relevant to an ordinary consumer's use of or experience with the product and are available to the ordinary consumer. This evaluation must have included an examination or testing of the product at least as extensive as someone with the same degree of expertise would normally need to conduct in order to support the conclusions presented in the endorsement. To the extent that the advertisement implies that the endorsement was based upon a comparison, such comparison must have been included in the expert's evaluation; and as a result of such comparison, the expert must have concluded that, with respect to those features on which he or she is expert and which are relevant and available to an ordinary consumer, the endorsed product is at least equal overall to the competitors' products. Moreover, where the net impression created by the endorsement is that the advertised product is superior to other products with respect to any such feature or features, then the expert must in fact have found such superiority. [See § 255.1(d) regarding the liability of endorsers.]

Example 1: An endorsement of a particular automobile by one described as an "engineer" implies that the endorser's professional training and experience are such that he is well acquainted with the design and performance of automobiles. If the endorser's field is, for example, chemical engineering, the endorsement would be deceptive.

Example 2: An endorser of a hearing aid is simply referred to as "Doctor" during the course of an advertisement. The ad likely implies that the endorser is a medical doctor with substantial experience in the area of hearing. If the endorser is not a medical doctor with substantial experience in audiology, the endorsement would likely be deceptive. A non-medical "doctor" (*e.g.*, an individual with a Ph.D. in exercise physiology) or a physician without substantial experience in the area of hearing can endorse the product, but if the endorser is referred to as "doctor," the advertisement must make clear the nature and limits of the endorser's expertise.

Example 3: A manufacturer of automobile parts advertises that its products are approved by the "American Institute of Science." From its name, consumers would infer that the "American Institute of Science" is a bona fide independent testing organization with expertise in judging automobile parts and that, as such, it would not approve any automobile part without first testing its efficacy by means of valid scientific methods. If the American Institute of Science is not such a bona fide independent testing organization

(e.g., if it was established and operated by an automotive parts manufacturer), the endorsement would be deceptive. Even if the American Institute of Science is an independent bona fide expert testing organization, the endorsement may nevertheless be deceptive unless the Institute has conducted valid scientific tests of the advertised products and the test results support the endorsement message.

Example 4: A manufacturer of a non-prescription drug product represents that its product has been selected over competing products by a large metropolitan hospital. The hospital has selected the product because the manufacturer, unlike its competitors, has packaged each dose of the product separately. This package form is not generally available to the public. Under the circumstances, the endorsement would be deceptive because the basis for the hospital's choice – convenience of packaging – is neither relevant nor available to consumers, and the basis for the hospital's decision is not disclosed to consumers.

Example 5: A woman who is identified as the president of a commercial “home cleaning service” states in a television advertisement that the service uses a particular brand of cleanser, instead of leading competitors it has tried, because of this brand's performance. Because cleaning services extensively use cleansers in the course of their business, the ad likely conveys that the president has knowledge superior to that of ordinary consumers. Accordingly, the president's statement will be deemed to be an expert endorsement. The service must, of course, actually use the endorsed cleanser. In addition, because the advertisement implies that the cleaning service has experience with a reasonable number of leading competitors to the advertised cleanser, the service must, in fact, have such experience, and, on the basis of its expertise, it must have determined that the cleaning ability of the endorsed cleanser is at least equal (or superior, if such is the net impression conveyed by the advertisement) to that of leading competitors' products with which the service has had experience and which remain reasonably available to it. Because in this example the cleaning service's president makes no mention that the endorsed cleanser was “chosen,” “selected,” or otherwise evaluated in side-by-side comparisons against its competitors, it is sufficient if the service has relied solely upon its accumulated experience in evaluating cleansers without having performed side-by-side or scientific comparisons.

Example 6: A medical doctor states in an advertisement for a drug that the product will safely allow consumers to lower their cholesterol by 50 points. If the materials the doctor reviewed were merely letters from satisfied consumers or the results of a rodent study, the endorsement would likely be deceptive because those materials are not what others with the same degree of expertise would consider adequate to support this conclusion about the product's safety and efficacy.

§ 255.4 Endorsements by organizations.

Endorsements by organizations, especially expert ones, are viewed as representing the judgment of a group whose collective experience exceeds that of any individual member, and whose judgments are generally free of the sort of subjective factors that vary from individual to individual.

Therefore, an organization's endorsement must be reached by a process sufficient to ensure that the endorsement fairly reflects the collective judgment of the organization. Moreover, if an organization is represented as being expert, then, in conjunction with a proper exercise of its

expertise in evaluating the product under § 255.3 (expert endorsements), it must utilize an expert or experts recognized as such by the organization or standards previously adopted by the organization and suitable for judging the relevant merits of such products. [See § 255.1(d) regarding the liability of endorsers.]

Example: A mattress seller advertises that its product is endorsed by a chiropractic association. Because the association would be regarded as expert with respect to judging mattresses, its endorsement must be supported by an evaluation by an expert or experts recognized as such by the organization, or by compliance with standards previously adopted by the organization and aimed at measuring the performance of mattresses in general and not designed with the unique features of the advertised mattress in mind.

§ 255.5 Disclosure of material connections.

When there exists a connection between the endorser and the seller of the advertised product that might materially affect the weight or credibility of the endorsement (*i.e.*, the connection is not reasonably expected by the audience), such connection must be fully disclosed. For example, when an endorser who appears in a television commercial is neither represented in the advertisement as an expert nor is known to a significant portion of the viewing public, then the advertiser should clearly and conspicuously disclose either the payment or promise of compensation prior to and in exchange for the endorsement or the fact that the endorser knew or had reason to know or to believe that if the endorsement favored the advertised product some benefit, such as an appearance on television, would be extended to the endorser. Additional guidance, including guidance concerning endorsements made through other media, is provided by the examples below.

Example 1: A drug company commissions research on its product by an outside organization. The drug company determines the overall subject of the research (*e.g.*, to test the efficacy of a newly developed product) and pays a substantial share of the expenses of the research project, but the research organization determines the protocol for the study and is responsible for conducting it. A subsequent advertisement by the drug company mentions the research results as the “findings” of that research organization. Although the design and conduct of the research project are controlled by the outside research organization, the weight consumers place on the reported results could be materially affected by knowing that the advertiser had funded the project. Therefore, the advertiser’s payment of expenses to the research organization should be disclosed in this advertisement.

Example 2: A film star endorses a particular food product. The endorsement regards only points of taste and individual preference. This endorsement must, of course, comply with § 255.1; but regardless of whether the star’s compensation for the commercial is a \$1 million cash payment or a royalty for each product sold by the advertiser during the next year, no disclosure is required because such payments likely are ordinarily expected by viewers.

Example 3: During an appearance by a well-known professional tennis player on a television talk show, the host comments that the past few months have been the best of her career and during this time she has risen to her highest level ever in the rankings. She responds by attributing the improvement in her game to the fact that she is seeing the ball

better than she used to, ever since having laser vision correction surgery at a clinic that she identifies by name. She continues talking about the ease of the procedure, the kindness of the clinic's doctors, her speedy recovery, and how she can now engage in a variety of activities without glasses, including driving at night. The athlete does not disclose that, even though she does not appear in commercials for the clinic, she has a contractual relationship with it, and her contract pays her for speaking publicly about her surgery when she can do so. Consumers might not realize that a celebrity discussing a medical procedure in a television interview has been paid for doing so, and knowledge of such payments would likely affect the weight or credibility consumers give to the celebrity's endorsement. Without a clear and conspicuous disclosure that the athlete has been engaged as a spokesperson for the clinic, this endorsement is likely to be deceptive. Furthermore, if consumers are likely to take away from her story that her experience was typical of those who undergo the same procedure at the clinic, the advertiser must have substantiation for that claim.

Assume that instead of speaking about the clinic in a television interview, the tennis player touts the results of her surgery – mentioning the clinic by name – on a social networking site that allows her fans to read in real time what is happening in her life. Given the nature of the medium in which her endorsement is disseminated, consumers might not realize that she is a paid endorser. Because that information might affect the weight consumers give to her endorsement, her relationship with the clinic should be disclosed.

Assume that during that same television interview, the tennis player is wearing clothes bearing the insignia of an athletic wear company with whom she also has an endorsement contract. Although this contract requires that she wear the company's clothes not only on the court but also in public appearances, when possible, she does not mention them or the company during her appearance on the show. No disclosure is required because no representation is being made about the clothes in this context.

Example 4: An ad for an anti-snoring product features a physician who says that he has seen dozens of products come on the market over the years and, in his opinion, this is the best ever. Consumers would expect the physician to be reasonably compensated for his appearance in the ad. Consumers are unlikely, however, to expect that the physician receives a percentage of gross product sales or that he owns part of the company, and either of these facts would likely materially affect the credibility that consumers attach to the endorsement. Accordingly, the advertisement should clearly and conspicuously disclose such a connection between the company and the physician.

Example 5: An actual patron of a restaurant, who is neither known to the public nor presented as an expert, is shown seated at the counter. He is asked for his “spontaneous” opinion of a new food product served in the restaurant. Assume, first, that the advertiser had posted a sign on the door of the restaurant informing all who entered that day that patrons would be interviewed by the advertiser as part of its TV promotion of its new soy protein “steak.” This notification would materially affect the weight or credibility of the patron's endorsement, and, therefore, viewers of the advertisement should be clearly and conspicuously informed of the circumstances under which the endorsement was obtained.

Assume, in the alternative, that the advertiser had not posted a sign on the door of the restaurant, but had informed all interviewed customers of the “hidden camera” only after interviews were completed and the customers had no reason to know or believe that their response was being recorded for use in an advertisement. Even if patrons were also told that they would be paid for allowing the use of their opinions in advertising, these facts need not be disclosed.

Example 6: An infomercial producer wants to include consumer endorsements for an automotive additive product featured in her commercial, but because the product has not yet been sold, there are no consumer users. The producer’s staff reviews the profiles of individuals interested in working as “extras” in commercials and identifies several who are interested in automobiles. The extras are asked to use the product for several weeks and then report back to the producer. They are told that if they are selected to endorse the product in the producer’s infomercial, they will receive a small payment. Viewers would not expect that these “consumer endorsers” are actors who were asked to use the product so that they could appear in the commercial or that they were compensated. Because the advertisement fails to disclose these facts, it is deceptive.

Example 7: A college student who has earned a reputation as a video game expert maintains a personal weblog or “blog” where he posts entries about his gaming experiences. Readers of his blog frequently seek his opinions about video game hardware and software. As it has done in the past, the manufacturer of a newly released video game system sends the student a free copy of the system and asks him to write about it on his blog. He tests the new gaming system and writes a favorable review. Because his review is disseminated via a form of consumer-generated media in which his relationship to the advertiser is not inherently obvious, readers are unlikely to know that he has received the video game system free of charge in exchange for his review of the product, and given the value of the video game system, this fact likely would materially affect the credibility they attach to his endorsement. Accordingly, the blogger should clearly and conspicuously disclose that he received the gaming system free of charge. The manufacturer should advise him at the time it provides the gaming system that this connection should be disclosed, and it should have procedures in place to try to monitor his postings for compliance.

Example 8: An online message board designated for discussions of new music download technology is frequented by MP3 player enthusiasts. They exchange information about new products, utilities, and the functionality of numerous playback devices. Unbeknownst to the message board community, an employee of a leading playback device manufacturer has been posting messages on the discussion board promoting the manufacturer’s product. Knowledge of this poster’s employment likely would affect the weight or credibility of her endorsement. Therefore, the poster should clearly and conspicuously disclose her relationship to the manufacturer to members and readers of the message board.

Example 9: A young man signs up to be part of a “street team” program in which points are awarded each time a team member talks to his or her friends about a particular advertiser’s products. Team members can then exchange their points for prizes, such as concert tickets or electronics. These incentives would materially affect the weight or credibility of the team member’s endorsements. They should be clearly and conspicuously disclosed, and the advertiser should take steps to ensure that these disclosures are being provided.

BUSINESS / MEDIA

FTC Issued Warnings to 45 Celebrities Over Unclear Instagram Posts

The letters were meant to educate influencers and brands on FTC's endorsement guidelines.

By [Alexandra Steigrad](#) on May 8, 2017



The power of [social media](#) as a marketing tool has not escaped brands, celebrities — or The Federal Trade Commission.

Last month the FTC [issued warnings](#) to celebrities who plugged products on their [Instagram](#) accounts without clearly identifying their relationships with brands. The letters were meant to “educate” the celebrities on how to post without violating the organization’s disclosure guidelines.

WWD has obtained the 90 letters sent to 45 celebrities, their agents and the brands they were publicizing. Top celebrities included Sean Combs, [Naomi Campbell](#), Sofia Vergara, [Heidi Klum](#), [Victoria Beckham](#), Allen Iverson, Lindsay Lohan, [Kourtney Kardashian](#), Scott Disick, Zendaya, Jennifer Lopez and Akon. In the fashion, beauty and retail space, letters were sent to Adidas, [Chanel](#), Lorac Cosmetics, Chiara Ferragni Collection, Cabela’s, Johnson & Johnson, Eos Products, Matisse Footwear, Yves [Saint Laurent](#) and Puma. Many of the posts in question have been taken down by the influencers either at the request of the brands or their agents. A full list of celebrities and brands appears below.

The FTC said it sent out similar letters to each influencer to “call attention” to the post in question. Each letter reads: “The FTC’s Endorsement Guides state that if there is a ‘material connection’ between the endorser and the marketer of a product — in other words, a connection that might affect the weight or credibility that consumers give the endorsement — that connection should be clearly and conspicuously disclosed, unless the connection is already clear from the context of the communication containing the endorsement. Material connections could consist of a business or family relationship, monetary payment, or the provision of free products to the endorser.”

The organization explained that disclosures, which commonly takes the form of #ad in a post, should be “clear” and “conspicuous” and use “unambiguous language” that “stands out.” The FTC cited cases in which disclosures appeared in captions at the bottom of a post, and were only found if consumers clicked on the “more” button to reveal the full text. Multiple hashtags, tags and links also were frowned upon, as they obscure the disclosure.

For further clarity, the FTC enclosed two endorsement guides, which address ethical issues about credibility and whether accepting free products means influencers need to disclose that

relationship to fans. In most cases, the FTC tends to err on the side of disclosure, even for athletes who are known ambassadors of brands.

The issue becomes murky when influencers are merely sharing that they are a fan of a particular product or brand. To that, the FTC says: “If you write about how much you like something you bought on your own and you’re not being rewarded, you don’t have to worry.”

But in a handful of the cases, the FTC still insists on clarity. For instance, [Victoria Beckham](#), who was sent a letter, posted about the brand Lancer Skin Care. The designer is pictured with its Contour Décolleté product and writes: “Loving this new contour by Décolleté by my friend @drlancerrx kisses from Los Angeles us X vb.”

Here, the FTC advocates for Beckham to disclose whether she has a financial or other business relationship with Lancer Skin Care, even though she refers to Dr. Lancer as a friend. Lancer aside, such posts may be difficult to police and create a slippery slope where influencers, brands and [perhaps media companies](#) and editors are put under a microscope.

Influencer

Jen Selter and Nicky Jam
 Sean Combs
 Shay Mitchell
 Ciara and Dorothy Wang
 Luke Bryan
 Kristin Cavallari
 Lucy Hale
[Naomi Campbell](#)
 Giuliana Rancic
 Sofia Vergara
[Heidi Klum](#)
 Rach Parcell
 JWOWW and Jamie Lynn Spears
 Maci Bookout McKinney
 Nicole Polizzi and Tiona Fernan

Letter recipient (Brand)

Mark King, president of Adidas NA
 Hal Kravitz, ceo Aquahydrate
 John Nosek, president of Kao USA
 Jeremy Joseph, president and general counsel of Buscemi
 Thomas L. Millner, ceo Cabela’s
 John Galantic, president and chief operating officer [Chanel](#) USA
 Riccardo Pozzoli, cofounder of Chiara Ferragni Collection
 Albert Bitton, cofounder The Clean ProgramCorp.
 Alex Gorsky, chairman and ceo of Johnson & Johnson
 Dana Gordon, ceo Dana Rebecca Designs
 Nigel Travis, ceo Dunkin’ Brands Group
 Sherry Jhavar, director of Smooth Strategies, Eos Products LLC
 Daniel and Michael Broukhim, coceos, cofounders of FabFitFun
 Joede Grant, owner J Gran Enterprise LLC
 Jack Ross, chairman, ceo Synergy CHC Corp.

Amber Rose	Samira Asemanfar and Melody Godfred of Fred and Far
Vanessa Hudgens	Anthony Fletcher, ceo of Nature Delivered
Valentina Vignali	James Hill, founder of Hairburst Limited
Lilly Ghalichi	Leyla Milani-Khoshbin, Khosh Milani Enterprises
Caroline Manzo	Dominik Richter, ceo of Hello Fresh AG
Allen Iverson	Rilwan Hassan, IO Moonwalkers Inc.
Behati Prinsloo	Josie Maran, founder and chief empowerment officer of Josie Maran Cosmetics
Anna Petrosian	David Sultineau, ceo of Kendo Brands Inc.
Shay Mitchell	Brian Driscoll, ceo Diamond Foods Inc.
Victoria Beckham	Tracey Sameyah, ceo and Harold Lancer of Lancer Skin Care LLC
Kristin Cavallari	Tim McMeekan, ceo of Lorac Cosmetics
Chelsea Houska	Aihui Ong, ceo of EdgiLife Media Inc.
Troian Bellisario	Michael Katz, owner of Matisse Footwear
Nina Agdal	Andy Benson, vice president of CytoSport Inc.
Vanessa Hudgens	Brian Goldner, ceo of Hasbro Inc.
Emily Ratajkowski and Ashley Benson	Maria Hatzistefanis, ceo of Rodial Limited
Denice Moberg	Hugh McGuire, ceo of Glanbia Performance Nutrition Inc.
James Harrison	Ian Danney, owner of Optimum EFX Formulations LLC
Scott Disick	Jake Munday, co-owner and director of Pearly Whites Australia
Lindsay Lohan	Ferit Rahvanci, manager of Pinner USA Inc.
<u>Kourtney Kardashian</u>	Cheryl Bachelder, ceo of Popeyes Louisiana Kitchen Inc.
Zendaya and Bella Thorne	Jay Piccola, president and GM of Puma North America
Sophia Bush	Whitney Tingle, ceo of Sakara Life
Massy Arias	Richelieu Dennis, ceo of Sundial Brands LLC
Farrah Abraham	Walker Williams, ceo of Teespring Inc.
Lisa Rinna	Jana Toohey, president of ToGoSpa LLC
Troian Bellisario	Joshua Koudelka, owner of Understated Leather
Akon (Aliaune Damala Badara Thiam) and Jennifer Lopez	Alexander Mechetin, ceo of JSC Synergy Group
Lucy Hale	Kate Voegelé, We The Dreamers LLC
Vanessa Lachey	Brant Cryder, president of Yves <u>Saint Laurent</u> North America



FTC Staff Reminds Influencers and Brands to Clearly Disclose Relationship

Commission aims to improve disclosures in social media endorsements

Share This Page

FOR RELEASE

April 19, 2017

TAGS: [Bureau of Consumer Protection](#) | [Consumer Protection](#) | [Advertising and Marketing](#) | [Online Advertising and Marketing](#)

After reviewing numerous Instagram posts by celebrities, athletes, and other influencers, Federal Trade Commission staff recently sent out more than 90 letters reminding influencers and marketers that influencers should clearly and conspicuously disclose their relationships to brands when promoting or endorsing products through social media.

The letters were informed by petitions filed by Public Citizen and affiliated organizations regarding influencer advertising on Instagram, and Instagram posts reviewed by FTC staff. They mark the first time that FTC staff has reached out directly to educate social media influencers themselves.

The FTC's Endorsement Guides provide that if there is a "material connection" between an endorser and an advertiser – in other words, a connection that might affect the weight or credibility that consumers give the endorsement – that connection should be clearly and conspicuously disclosed, unless it is already clear from the context of the communication. A material connection could be a business or family relationship, monetary payment, or the gift of a free product. Importantly, the Endorsement Guides apply to both marketers and endorsers.

In addition to providing background information on when and how marketers and influencers should disclose a material connection in an advertisement, the letters each addressed one point specific to Instagram posts -- consumers viewing Instagram posts on mobile devices typically see only the first three lines of a longer post unless they click "more," which many may not do. The staff's letters informed recipients that when making endorsements on Instagram, they should disclose any material connection above the "more" button.

The letters also noted that when multiple tags, hashtags, or links are used, readers may just skip over them, especially when they appear at the end of a long post – meaning that a disclosure placed in such a string is not likely to be conspicuous.

Some of the letters addressed particular disclosures that are not sufficiently clear, pointing out that many consumers will not understand a disclosure like “#sp,” “Thanks [Brand],” or “#partner” in an Instagram post to mean that the post is sponsored.

The staff’s letters were sent in response to a sample of Instagram posts making endorsements or referencing brands. In sending the letters, the staff did not predetermine in every instance whether the brand mention was in fact sponsored, as opposed to an organic mention.

In addition to the Endorsement Guides, the FTC has previously addressed the need for endorsers to adequately disclose connections to brands through law enforcement actions and the staff’s business education efforts. The staff also issued [FTC’s Endorsement Guides: What People are Asking](#), an informal business guidance document that answers frequently asked questions. The staff’s letters to endorsers and brands enclosed copies of both guidance documents. The FTC is not publicly releasing the letters or the names of the recipients at this time.

The Federal Trade Commission works to promote competition, and [protect and educate consumers](#). You can [learn more about consumer topics](#) and file a [consumer complaint online](#) or by calling 1-877-FTC-HELP (382-4357). Like the FTC on [Facebook](#), follow us on [Twitter](#), read our [blogs](#) and [subscribe to press releases](#) for the latest FTC news and resources.

Contact Information

MEDIA CONTACT:

Mitchell J. Katz,
Office of Public Affairs
202-326-2161

STAFF CONTACTS:

Michael Ostheimer,
Bureau of Consumer Protection
202-326-2699

Mamie Kresses,
Bureau of Consumer Protection
202-326-2070



ftc.gov

{Date}

{Address}

Dear {Influencer}:

The Federal Trade Commission is the nation’s consumer protection agency. As part of our consumer protection mission, we work to educate marketers about their responsibilities under truth-in-advertising laws and standards, including the FTC’s Endorsement Guides.¹

I am writing regarding your attached Instagram post endorsing {product or service}.² You posted a picture of {description of picture}. You wrote, “{quotation from Instagram post}.”

The FTC’s Endorsement Guides state that if there is a “material connection” between an endorser and the marketer of a product – in other words, a connection that might affect the weight or credibility that consumers give the endorsement – that connection should be clearly and conspicuously disclosed, unless the connection is already clear from the context of the communication containing the endorsement. Material connections could consist of a business or family relationship, monetary payment, or the provision of free products to the endorser.

The Endorsement Guides apply to marketers and endorsers. [If there is a material connection between you and {Marketer}, that connection should be clearly and conspicuously disclosed in your endorsements.] *or* [It appears that you have a business relationship with {Marketer}. Your material connection to that company should be clearly and conspicuously disclosed in your endorsements.] To make a disclosure both “clear” and “conspicuous,” you should use unambiguous language and make the disclosure stand out. Consumers should be able to notice the disclosure easily, and not have to look for it. For example, consumers viewing posts in their Instagram streams on mobile devices typically see only the first three lines of a longer post unless they click “more,” and many consumers may not click “more.” Therefore, you should disclose any material connection above the “more” button. In addition, where there are multiple tags, hashtags, or links, readers may just skip over them, especially where they appear at the end of a long post.

¹ The Endorsement Guides are published in 16 C.F.R. Part 255.

² The post is available at {URL}.

If you are endorsing the products or services of any marketers with whom you have a material connection, you may want to review the enclosed FTC staff publication, *The FTC Endorsement Guides: What People are Asking*. I'm also enclosing a copy of the *Endorsement Guides* themselves. (Both documents are available online at business.ftc.gov.)

If you have any questions, please contact Mamie Kresses at (202) 326-2070 or mkresses@ftc.gov. Thank you.

Very truly yours,

Mary K. Engle
Associate Director
Division of Advertising Practices

{Date}

{Address}

Dear {Influencer}:

The Federal Trade Commission is the nation’s consumer protection agency. As part of our consumer protection mission, we work to educate marketers about their responsibilities under truth-in-advertising laws and standards, including the FTC’s Endorsement Guides.¹

I am writing regarding your attached Instagram post endorsing {product or service}.² You posted a picture of {description of picture}. You wrote, “{quotation from Instagram post}.”

The FTC’s Endorsement Guides state that if there is a “material connection” between an endorser and the marketer of a product – in other words, a connection that might affect the weight or credibility that consumers give the endorsement – that connection should be clearly and conspicuously disclosed, unless the connection is already clear from the context of the communication containing the endorsement. Material connections could consist of a business or family relationship, monetary payment, or the provision of free products to the endorser.

The Endorsement Guides apply to marketers and endorsers. [If there is a material connection between you and {Marketer}, that connection should be clearly and conspicuously disclosed in your endorsements.] *or* [It appears that you have a business relationship with {Marketer}. Your material connection to that company should be clearly and conspicuously disclosed in your endorsements.] To make a disclosure both “clear” and “conspicuous,” you should use unambiguous language and make the disclosure stand out. Consumers should be able to notice the disclosure easily, and not have to look for it. For example, consumers viewing posts in their Instagram streams on mobile devices typically see only the first three lines of a longer post unless they click “more,” and many consumers may not click “more.” Therefore, you should disclose any material connection above the “more” button. In addition, where there are multiple tags, hashtags, or links, readers may just skip over them, especially where they appear at the end of a long post.

¹ The Endorsement Guides are published in 16 C.F.R. Part 255.

² The post is available at {URL}.

If you are endorsing the products or services of any marketers with whom you have a material connection, you may want to review the enclosed FTC staff publication, *The FTC Endorsement Guides: What People are Asking*. I'm also enclosing a copy of the *Endorsement Guides* themselves. (Both documents are available online at business.ftc.gov.)

If you have any questions, please contact Mamie Kresses at (202) 326-2070 or mkresses@ftc.gov. Thank you.

Very truly yours,

Mary K. Engle
Associate Director
Division of Advertising Practices

Online consignment changes the game for used goods

By [Molly Wood](#) and [Eliza Mills](#)

December 02, 2015 | 12:41 PM



Designer clothes line the racks at The RealReal, an online consignment shop that brings in millions in revenue. - Molly Wood/Marketplace

The new fashion season is here, and with holiday shopping in full swing, lots of people will be trading up, and maybe cleaning out their closets. Used clothing was once relegated to garage sales or Goodwill, but in recent years, online consignment businesses have cashed in on clothing cleanouts, creating a marketplace for old clothes, shoes, jewelry and accessories.

At The RealReal, a San Francisco–based luxury online resale site, the cast-offs include Prada, Gucci, Balenciaga, Cartier and Jimmy Choo. The warehouse is enormous and filled to the brim with millions of dollars in clothing and jewelry. Founder and CEO Julie Wainwright started The RealReal in 2011 because she believed luxury buyers would jump at an easy — and discreet — way to unload last season’s looks, and more mainstream shoppers would be eager to pick them up at a discount.

"Fifty percent of our consigners have never consigned before — so I would say we're actually changing the way that people look at the value of things in their home," Wainwright said.

For sellers looking for a return on the high-end goods they're looking to get rid of, The RealReal pays sellers up to 70 percent of the sale price, and accepts items Fedex-ed to their warehouse through a free online download system. For consignors with the most valuable goods, the company will dispatch one of its luxury managers to individual homes for white glove service.



Designer shoes packed in boxes at the RealReal offices. (Molly Wood/Marketplace)

And the clothes and jewelry sold through the site moves fast, rotating out about once every two weeks. The RealReal's cut — about 20-40 percent of each item sold, depending on its value — will bring in around \$200 million this year in revenue and should be profitable next year.

That is, if the competition in second-hand retail doesn't get too stiff. Online consignment has become a hugely competitive arena online. Sites and apps like ThredUp, SnobSwap, Tradesy and of course, The RealReal itself, has pulled in millions of dollars in funding. According to Matthew

Wong, an analyst at CB Insights, the market for secondhand retail "definitely looks a bit bloated" and that there will likely be "opportunities for consolidation and acquisitions later on."

Wong said that a few companies have risen to the top, like The RealReal and its lower-end competitor, ThredUp, with over \$80 million in funding each. But the funding is not a guarantee of success, and differentiation will be key in maintaining a steady stream of business.

The RealReal sets itself apart by aiming for total authenticity and luxury — their staff includes authenticators and gemologists who examine the valuable goods as they enter their warehouses and photographers who stage and shoot the clothing.

At The RealReal's offices, Meaghan Wallace, a gemologist at The RealReal, authenticates a vintage sapphire and diamond bracelet and values it at \$18,000 — a steal, since she said the original owner paid \$45,000.

The bracelet will be photographed, listed online and put back into the fingerprint-sensored vault with The RealReal's other jewels to stay safe until it sells.



One of the many expensive jewelry pieces at RealReal. - Molly Wood/Marketplace

<http://www.marketplace.org/2015/12/02/business/online-consignment-changes-game-used-goods>

The RealReal

Company Overview

The RealReal is the leader in authenticated luxury consignment with a certified expert behind every single item. The consignment company reinvented luxury resale and has changed how people think about and consume luxury goods. The RealReal provides the largest selection of pre-owned authenticated luxury items including women's and men's fashion, fine jewelry & watches, and fine art & home. Consignors earn up to 70% of the sale price and items sell quickly. The company also has Luxury Consignment offices in 6 US cities that offer free fine jewelry and watch valuations from certified gemologists, as well as a white glove consignment service in every city. The RealReal is a leader in the circular economy and an innovator in sustainable luxury.

Fast Facts

- Founded in 2011 by seasoned tech CEO, Julie Wainwright
- Member base: **6 million members / shoppers**
- Sold and shipped over **5 million** luxury items to date
- **200,000 social followers** across Instagram, FB, and Twitter
- **RealBook mobile app** directory of sold items with sale prices
 - To download visit: www.therealreal.com/mobile
- Luxury goods in watches, women's and men's fashion; fine jewelry & home
- Offices: San Francisco, New York City, Los Angeles, Chicago, DC, Dallas
- Watch and jewelry valuation offices in midtown Manhattan, San Francisco, Los Angeles, Chicago, DC, and Dallas
 - Contact: valuation@therealreal.com
- White Glove service in **30 U.S. markets (100 Luxury Managers)**
- International shipping to **61 countries**
- Distribution Centers: **300,000+ sq feet**
- San Francisco, New Jersey, and Los Angeles
- Venture Funding: **\$173 million as of June 6**
- 900 Employees
- 50% of consignors have never consigned before - we have removed all the friction - it's easy and smart and now people have realized there's a way to get money back on items they have invested in.
- The RealReal is taking the top off eBay and the bottom off Christie's and Sotheby's

Julie Wainwright, Founder & CEO of The RealReal

Leading luxury consignment site The RealReal is changing the way people shop. By offering consignors liquidity on their luxury items, consignor's buying patterns have changed, as they now consider the resale value of luxury items before buying new items. The RealReal is the only company that provides effortless consignment, by offering free in-home pick up and handling all the work on the consignor's behalf, from authentication through to shipping. For customers, The RealReal guarantees that the pre-owned luxury goods it sells are authentic at an amazing value while providing a full customer service experience including customer returns.

About the Founder - Julie was an e-commerce pioneer as CEO of Reel.com in 1997 and Pets.com in 1999. In 2017, Julie was named to TechCrunch's 'Women Who Had a Great 2016' and named by SF Business Times as one of the most influential women of the year. In 2016, Julie and The RealReal were awarded the Innovation in Retail E-commerce award by the prestigious Fashion Group International. In 2015, Julie was named to the Business of Fashion 500 list, featuring the most influential people shaping

the global fashion industry today. In the same year, The RealReal was awarded the “Game Changer” award by W Magazine and Decoded Fashion.

In 2014, Julie was named one of TechCrunches "40 Over 40" Silicon Valley entrepreneurs, and was recognized by The San Francisco Business Times as one of the most admired CEOs of the year. She is a frequent speaker at industry events like Vanity Fair New Establishment Summit, Decoded Fashion, and Financial Times, along with top universities like Purdue and Stanford University. She actively supports dozens of local and national non-profits focused on women, children and the arts.

Rati Levesque, Chief Merchant of The RealReal

Rati Levesque, Chief Merchant of The RealReal, is responsible for the merchandising, editorial and creative vision of the company. In her role she oversees all creative development, product merchandising, authentication, and customer experience. Rati joined The RealReal Founder and CEO Julie Wainwright in 2011 as the company's first employee and a catalyst to bringing Julie's vision of a new way to buy and sell consigned luxury goods to life. Prior to joining The RealReal, Rati launched her first entrepreneurial endeavor with the fashion-forward Russian Hill boutique, Anica. Setting out to fill the void of avant-garde designers in the city, Anica acquired a significant following, especially for the store's luxury consignment selection. Prior to that, she worked in the financial industry, following her graduation from the University of California, Santa Cruz where she received a degree in Economics.

Rati is featured prominently in fashion publications like Fashionista, The Coveteur, ELLE, and more, offering expertise on all things luxury and consignment. She spoke at Fortune's 2016 Most Powerful Women Next Gen Summit and was recognized by Luxury Daily as one of their 2015 Luxury Women to Watch. She was also part of the ShopStyle Advisory Board from 2015 - 2016. She resides in San Francisco with her husband and two children.

Press Contact

Natalie Seufferlein

natalie.seufferlein@therealreal.com

AUTHENTICITY

THE REALREAL POLICY ON AUTHENTICITY

Authenticity is the cornerstone of The RealReal. We staff trained, in-house professionals including gemologists, horologists, art appraisers and apparel experts who work to ensure that every item sold is 100% authentic and in beautiful condition.

MULTI-POINT INSPECTION AND EVALUATION

All items are put through a multi-point, brand-specific authentication process by a trained team of luxury experts headed by our Senior Director of Authentication & Brand Compliance before they are accepted for consignment. We inspect all goods for appropriate brand markings, date codes, serial tags and hologram stickers. Everything passes through our strict authenticity tests before it is curated into daily sales. Our fine jewelry and watches are authenticated and appraised by our gemologists and horologists and each piece comes with a valuation certificate. Art items are thoroughly researched and validated by our team of fine art specialists.

The RealReal's authentication process is unique to The RealReal and independent of any brands. Brands identified are not involved in the authentication of the products being sold, and none of the brands sold assume any responsibility for any products purchased from or through the website. Brands sold on The RealReal are not partnered or affiliated with The RealReal in any manner. However, The RealReal fully cooperates with brands and state and federal agencies seeking to track down the source of counterfeit items, which includes revealing the contact information of consignors submitting counterfeit goods.

GOODS DETERMINED TO BE COUNTERFEIT

The RealReal does not accept fake or counterfeit merchandise of any kind. If we suspect that a submitted consignment is not authentic we will contact the consignor in an effort to establish the items authenticity. **Items The RealReal determines are counterfeit will not be returned to the consignor and will be destroyed.**

Amazon's Chinese counterfeit problem is getting worse

Ari Levy

Friday, 8 Jul 2016

[Amazon.com](#) is hard at work promoting next week's [Prime Day](#) and the more than 100,000 deals available to subscribers. As with all things Amazon, it's intended to be a major party for consumers.

But longtime Amazon sellers like Jamie Whaley are in no mood to celebrate.

A licensed nurse, Whaley started a bedding business on Amazon that reached \$700,000 in annual sales within three years. Her patented product called BedBand consists of a set of shock cords, clamps and locks designed to keep fitted bed sheets in place.

Whaley and her husband found quite an audience, selling up to 200 units a day for \$13.99 a set. BedBand climbed into the top 200 selling products in the home and kitchen category. That was 2013.

By mid-2015, the business was in a tailspin. Revenue plummeted by half and Whaley was forced to lay off eight employees. Her sheet fastener had been copied by a legion of mostly Chinese knockoffs that undercut BedBand on price and jumped the seller ranks by obtaining scores of reviews that watchdog site [Fakespot.com](#) determined were inauthentic and "harmful for real consumers."

"Toe to toe we'll compete with anybody," said Whaley, who recently moved her family and a warehouse full of straps, clamps and cords from Texas to the mountains of Montana. "When you try to cheat or copy our products, it's a whole different story."

Whaley still counts on Amazon for 90 percent of her revenue but she's actively trying to drive traffic to her own [website](#) and partner with other retailers. She's lost all trust in Amazon.

Spend any time surveying Amazon sellers and Whaley's narrative will start sounding like the norm. In Amazon's quest to be the low-cost provider of everything on the planet, the website has morphed into the world's largest flea market — a chaotic, somewhat lawless, bazaar with unlimited inventory.

Always a problem, the counterfeiting issue has exploded this year, sellers say, following Amazon's effort to openly court Chinese manufacturers, weaving them intimately into the company's expansive logistics operation. Merchants are perpetually unsure of who or what may kill their sales on any given day and how much time they'll have to spend hunting down fakers.

[Facebook](#) and WhatsApp groups have formed for sellers to voice their complaints and strategize on potential fixes.

In May, CNBC.com [reported](#) on a Facebook group, now consisting of over 600 people, whose members have seen their designs for t-shirts, coffee mugs and iPhone cases show up on Amazon at a fraction of the price of the originals. The designers described it as a game of whack-a-mole, where fakes pop up more quickly than they're taken down.

It's not a topic you'll likely hear CEO [Jeff Bezos](#) discuss. Especially ahead of the [second annual Prime Day on Tuesday](#), when Amazon Prime members get access to new deals about every five minutes. During the inaugural event last year, consumers bought 398 items per second, even as social media blew up with [jokes](#) about the quality of the offers.

While Amazon's focus has always been on consumers, the company is plenty aware of emerging seller angst.

In early June, at an invitation-only event for about 300 of the top marketplace merchants, the company's senior vice president of seller services Sebastian

Gunningham was grilled by frustrated store owners, according to people with knowledge of the meeting.

During a fireside chat at Amazon's Seattle headquarters, Gunningham was asked repeatedly how the company was going to deal with the many ways that Chinese manufacturers were gaming the system, said the sources, who asked not to be named because attendees had to sign non-disclosure agreements.

An Amazon spokesperson declined to comment.

Outside merchants are a large and growing piece of the Amazon pie.

More than 40 percent of Amazon's unit sales now come through its third-party marketplace. Much of the expansion has occurred since Amazon started opening the floodgates to Chinese manufacturers, who previously had to count on middlemen, brands and private labels to reach global consumers.

Sales from Chinese-based sellers more than doubled in 2015 on Amazon's marketplaces, while the company's total revenue increased 20 percent. And recently, Amazon even registered with the [Federal Maritime Commission](#) to provide ocean freight, simplifying the process for Chinese companies to ship goods directly to Amazon fulfillment centers, cutting out costs and inefficiencies.

That's why you can get a box full of Chinese kitchen goods from a variety of sellers delivered in two days from a warehouse in Kentucky.

Critics say Amazon hasn't put the necessary checks in place to manage the influx of counterfeits.

To unsuspecting consumers, fake products can appear legitimate because of the Fulfillment by Amazon program, which lets manufacturers send their goods to

Amazon's fulfillment centers and hand over a bigger commission, gaining the stamp of approval that comes with an FBA tag.

Furthermore, Amazon's commingled inventory option bundles together products from different sellers, meaning that a counterfeit jacket could be sent to an Amazon facility by one merchant and actually sold by another.

"Amazon is making money hand over fist from counterfeiters, and they've done about as little as possible for as long as possible to address the issue," said Chris Johnson, an attorney at Johnson & Pham LLP, which focuses on intellectual property and brand enforcement and represents clients including Forever 21, [Adobe](#) and OtterBox. "Word is out in the counterfeit community that it's open season on Amazon."

It's not just niche brands like BedBand feeling the pain.

Birkenstock has seen dozens of stores at a time hawking its Arizona Sandal for \$79.99, a full \$20 below the retail price. The names of the online storefronts change all the time, one day including the monikers Silver Peak Wine Cellar and Ryan Hollifield and the next Keila*Knighthley and Bking sewneg.

Price + Shipping	Condition (Learn more)	Delivery	Seller Information	Buying Opti
\$76.99 + \$6.03 shipping + \$0.03 estimated tax	New Best Seller	• Arrives between July 28 - Aug. 15. • Domestic shipping rates and return policy.	Keila*Knighthley Just Launched (Seller Profile)	Sign in to buy
\$79.99 + \$5.07 shipping + \$0.03 estimated tax	New	• Arrives between July 15-22. • Ships from NL, Canada. • Domestic shipping rates and return policy.	caitlin stocum Just Launched (Seller Profile)	Sign in to buy
\$79.99 + \$5.07 shipping + \$0.03 estimated tax	New	• Arrives between July 15-22. • Ships from ON, Canada. • Domestic shipping rates and return policy.	Stephanie Vaughn Just Launched (Seller Profile)	Sign in to buy
\$79.99 + \$5.07 shipping + \$0.03 estimated tax	New	• Arrives between July 15-22. • Ships from QC, Canada. • Domestic shipping rates and return policy.	Adriana Zaldivar Just Launched (Seller Profile)	Sign in to buy
\$79.99 + \$5.07 shipping + \$0.03 estimated tax	New	• Arrives between July 15-22. • Ships from NB, Canada. • Domestic shipping rates and return policy.	Ann Braasch Just Launched (Seller Profile)	Sign in to buy
\$79.99 + \$5.07 shipping + \$0.03 estimated tax	New	• Arrives between July 15-22. • Ships from SK, Canada. • Domestic shipping rates and return policy.	John Clayton Just Launched (Seller Profile)	Sign in to buy
\$79.99 + \$5.07 shipping + \$0.03 estimated tax	New	• Arrives between July 15-22. • Ships from NB, Canada. • Domestic shipping rates and return policy.	carolrds Just Launched (Seller Profile)	Sign in to buy

Source: Amazon

Birkenstocks featured on Amazon

The only way to contact the sellers is by going to their storefront and clicking the "Ask a question" button. On a single day in mid-June, CNBC sent notes to seven sellers on the list, asking how they're able to price the product so cheaply. Every response was the same: "It is a secret."

Red flags are everywhere. [Michael Kors](#) has a signature [tote bag](#) listed as low as \$101 by multiple stores, compared to its \$198 [retail price](#). Canada Goose's highly popular [Expedition parka](#) sells for \$1,000 on its own site and is available for [under \\$650](#) on Amazon, a price that sellers of the brand say is too good to be true.

"As long as the logo looks legit, people assume you have that item," said a Canada Goose seller, who asked not to be named so as not to cause strain with Amazon.

Representatives from Birkenstock, Michael Kors and Canada Goose declined to comment.

Counterfeiting online is nothing new of course, particularly when it comes to commerce. [Alibaba](#), the Chinese e-retail giant, has been dealing with it since launching in 1999.

Some form of the word counterfeit shows up 30 times in Alibaba's latest annual report, and founder Jack Ma said in a speech last month in Hangzhou, China, that the fakes are of "better quality, better prices than the real products, the real names."

Amazon, by contrast, has tried to maintain its image as a clean venue and the trusted place for online buying. There's not a single use of the word counterfeit in its [2015 annual report](#), and only the last of its two dozen risk factors mentions potential liabilities associated with "fraudulent or unlawful activities of sellers."

Amazon rally



Investors certainly haven't expressed concern, bidding the stock up 69 percent in the past year. Amazon's market value of \$348 billion is equal to [Walgreens](#), Lowe's, Costco, [Target](#) and Macy's combined, after you tack on another \$66 billion. It's the sixth most valuable company in the U.S.

The Amazon story has always hinged on giving customers what they want and with top-notch service and speed. Walter Price, a portfolio manager at Allianz Global Investors, said it's no different with counterfeiting.

"If customers can verify that they've bought counterfeit goods, Amazon will push sellers to refund the purchase or they kick the sellers off the site," said Price, who also owns a stake in Alibaba. "Amazon does stick up for the consumer. They put the consumer first, not the merchant."

Sellers that want to cheat have any number of tools at their disposal. One issue that's enraged merchants is the proliferation of hijacked listings, where sellers suddenly see random names jump into their product page and start promoting the item for a cheaper price.

Judah Bergman has been selling on Amazon for two and a half years and his products include a jewelry line under the brand Steelttime. Other merchants have regularly

showed up in listings for his double-sided pearl earrings, offering them for under \$10, compared to the [\\$17.99](#) he charges.

"If you want to fight them, you won't have time to do anything else." -Judah Bergman, Amazon seller

While he's able to eventually get the hijackers removed, he loses sales in the process as customers opt for the lower priced option, and he's spent valuable time sending in takedown notices to Amazon.

Making matters worse, when buyers unhappy with the cheaper alternatives leave a bad review, it drags down Bergman's standing because the reviews are all thrown together.

"The next thing you know you've lost sales plus your good star rating," said Bergman. "If you want to fight them, you won't have time to do anything else."

Amazon has an [anti-counterfeiting](#) policy in place and responds to infringement notices, investigating and kicking off sellers who break the rules. But the fraudsters move fast, changing the names of their stores and relaunching as quickly as they're removed.

As a marketplace, Amazon isn't legally responsible for keeping counterfeit material off the site as long as it responds to complaints and takes action when it's brought to the company's attention.

Chris McCabe worked as an Amazon merchant account investigator for five years. Since 2014 he's been operating independently on the other side, helping third-party sellers navigate Amazon's rules and processes for staying compliant. He's often hired to help suspended sellers get reinstated.


McCabe said that Amazon's investment in preventing marketplace abuse, a task assigned to the transaction risk management team, is dwarfed by its focus on growth at the [AWS](#) division and other projects like the kindle and Amazon Studios.

"They've been reactive, not proactive," said McCabe, who's now based in the Boston area. "Amazon can't watch everyone all the time, and they don't pretend they can."

For Whaley and BedBand, the past 18 months have been a whirlwind since she discovered that copycats were all over her product.


Initially, knockoffs were using her patented shock cord functionality and ripping off her design, she said. Those blatant counterfeits have gone away, with most rival products now using generic elastic straps.

But there are plenty of other ways for competitors to game the system, such as manipulating product reviews.



Name
Adjustable Bed Sheet Fasteners
Suspender Set of 4 Black

Company
The Nyché Designs



There are indications of inauthentic/low quality reviews, you be the judge.

Grade

F

(62.0% low quality reviews detected)

Our analysis has detected product exchange for reviews. We believe these reviews are harmful for real consumers because of the inherent bias and our opinion reflects that.

Do you agree with this analysis? 👍 👎

Share this analysis (direct link) [🐦](#) [📘](#) [👤](#) [🐾](#) [🌐](#) [📺](#) [📺](#) [📺](#) [📺](#)

[Analysis Details](#) [Reviews Summary](#) [Reviews Word Cloud](#) [Discuss](#)

BedBand, which now sells for \$12.99, has over 3,750 reviews and a 4.5-star rating. In the sheet fastener category, it was the most popular item until late 2014, when a number of like products that Whaley had never seen started gathering hundreds of positive reviews, leapfrogging her in the ranking.

Today, after spending five years and \$60,000 on patents, BedBand is the number two seller in the category, behind a brand called Nyche Designs, whose top-selling product is priced at \$8.99. Nyche is based in China and registered a U.S. trademark in February, according to [Trademarkia](#).

Based on the quality of reviews, Whaley has good reason to be upset. Fakespot, an independent site that judges the validity of reviews, gives Nyche an F because it "detected product exchange for reviews." In other words, it paid for positive feedback.

Bed Band has an [A rating](#), according to Fakespot.

"We've never bought a review, and we've never taken the route to give products away for reviews," said Whaley.

Amazon has filed multiple lawsuits in the past year against sites that sell reviews, but Nyche's reviews still include language like this: "I received this item at discount in exchange for an honest and unbiased review."

Nyche did not respond to multiple requests for comment sent to the email address on its [website](#).

Make no mistake, Amazon's business is humming along. Prime is adding members by the truckload, more products are available with faster delivery rates, the Amazon Echo smart speaker is looking like the next killer product and there's even some profit to show investors, thanks largely to the fat margins at AWS

But for a brand built on trust, there are an awful lot of loopholes, and sellers are wondering if their gripes will ever become so problematic that Amazon can no longer sweep them under the rug.

"Amazon is setting up an environment where people feel like they have to shortcut and cheat," said Whaley. "The whole system is being manipulated, and people don't know it."

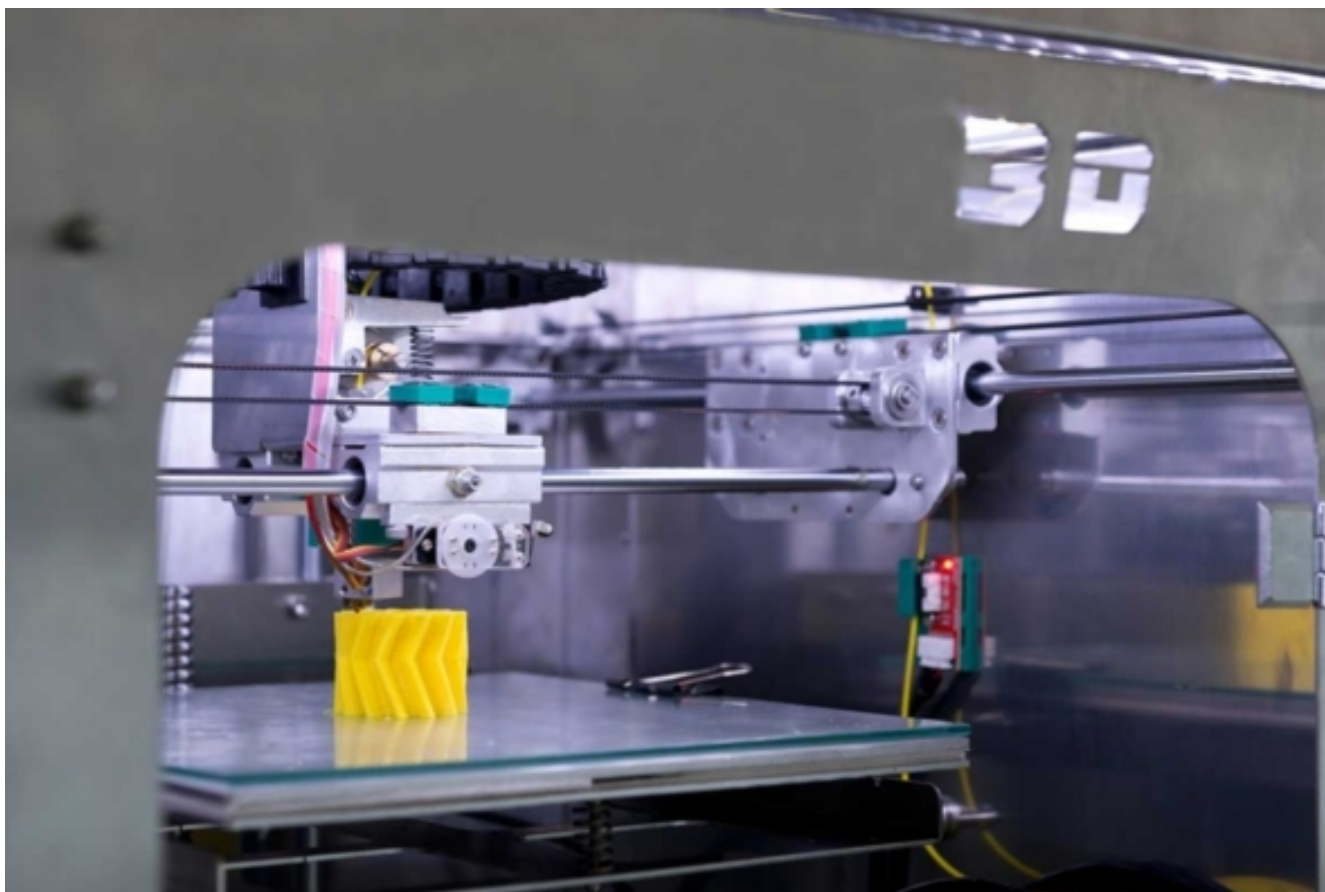
—*CNBC's Josh Lipton contributed to this report.*

TECH

How 3-D Printing Threatens Our Patent System

Patents will have even more trouble with 3-D copies than copyright law had with digital music sales

By Timothy Holbrook, Emory University, The Conversation on January 6, 2016



Credit: @iStock.com

Remember Napster or Grokster? Both services allowed users to share computer files—usually digital music—that infringed the copyrights for those songs.

Now imagine that, instead of music, you could download a physical object. Sounds like something from a sci-fi movie—push a button and there’s the item! But that scenario is already becoming a reality. With a 3D printer, someone can download a computer file, called a computer-aided design (CAD) file, that instructs the printer to make a physical, three-dimensional object.

Because CAD files are digital, they can be shared across the internet on file-sharing services, just like movies and music. Just as digital media challenged the copyright system with rampant copyright infringement, the patent system likely will encounter widespread infringement of patented inventions through 3D printing. The problem is, however, that the patent system is even more ill-equipped to deal with this situation than copyright law was, posing a challenge to a key component of our innovation system.

The factory at your fingertips

Technically called “additive manufacturing,” 3D printing from a CAD file allows someone to “print” physical items at home. The printer follows a file’s instructions to generate a physical object. The printer head releases tiny squirts of material that, layer by layer, build up into the item. 3D printers can create incredibly complex objects, such as rocket engine parts, human tissue, a bionic ear and even a functional gun.

The CAD files can be created by scanning in an object or by virtually

designing an object on the computer. Once you have what are essentially the blueprints, the object is then just a press of a button away. Of course, if that object is covered by a patent, then pushing that button results in patent infringement.

Potentially bypassing patent protection

Patents are actual documents issued by the federal government. They're awarded for inventions that are nontrivial advances in the state of the art. A patent allows the owner to prevent others from making, using, selling or importing the invention. These exclusive rights help keep competitors out of the market, allowing the patent owner to recover R&D costs. The owner also can use the patent to support efforts to commercialize the invention.

If people can evade the patent, however, then its value is reduced, undermining these important incentives. 3D printing presents this potential. It enables someone to “print” something that infringes a patent. Once someone prints the patented invention, they have “made” it, which violates the patent owner’s rights.

Each printed copy of an invention is a lost potential sale to the patent holder. But, to sue for infringement, the patent owner would need to be aware that someone is using a 3D printer to make the patented invention. And that’s a very tall order since these printers are widely dispersed across households and businesses.

Alternatively, patent owners could go after the people facilitating the infringement. The Patent Act permits a patent holder to sue parties who induce others to infringe. Potential inducers of patent infringement here could be the sellers of the 3D printers, someone

providing CAD files of the patented device, or websites that sell or share various CAD files that instruct the 3D printer to make the patented invention.

Copyright law similarly prohibits inducement of infringement. Grokster did not make the infringing copies of the music itself, but it certainly helped other people make infringing copies. The Supreme Court held that Grokster likely induced copyright infringement, and Grokster shut down. The same idea could apply in the patent context.

But there is a huge problem with this approach: inducement of patent infringement requires actual knowledge of the relevant patent. For music, everyone knows the songs are copyrighted. Not everyone is aware that a particular device is covered by a patent. There are hundreds of thousands of patents in existence. It's highly unlikely that potential inducers would have actual knowledge of every patent that could be infringed by use of a 3D printer.

For example, suppose a dentist develops a brilliant new form of plastic braces, and she patents it. Independently, another dentist with some computer savvy comes up with the same idea via a CAD file. He shares the file with his dentist friends with 3D printers, who then all begin printing the plastic braces. The dentist's friends start sharing the file with their friends, or someone places it on a file-sharing network. And so on. Anyone printing the braces is technically an infringer, but how can the patent owner find them all? And the dentist sharing his CAD file would have to be aware of the patent to be liable as an inducer, which may be unlikely.

Should the CAD files alone trigger infringement?

Will 3D printing undermine the innovation incentives the patent system is designed to provide? Potentially, but Professor Lucas Osborn of Campbell University School of Law and I have argued that courts can combat this problem by focusing on the CAD files, rather than the printed object.

Copyright provides a helpful contrast. Digital files themselves infringe. They are copies of the work. Not so in patent law. To infringe, one has to make a tangible version of the invention. But, if the infringing object is merely the press of a button away for someone with the CAD file and a 3D printer, should the CAD files themselves be viewed as digital patent infringement, similar to copyright law?

We argue that if someone sells a CAD file that prints a patented item, that should be considered infringing. The CAD file has value because of the patented invention, so the seller is appropriating the economic value of the invention.

But what if someone is not selling the CAD file? Instead, they just possess it. Should that be infringement, too? We think not. The patent system encourages others to design around existing patents, which is often done in a virtual space. If the CAD file itself would be viewed as infringement, then the system could lose such beneficial improvement efforts.

It is unclear if courts or Congress will act to address these issues. What is inevitable, however, is that 3D printing will prove challenging to our patent system. There is a great irony here. One of

the greatest innovations of our time may ultimately undermine a key engine of innovation, the patent system.

Timothy Holbrook does not work for, consult, own shares in or receive funding from any company or organization that would benefit from this article, and has disclosed no relevant affiliations beyond the academic appointment above.

This article was originally published on [The Conversation](#). Read [the original article](#).



Intellectual
Property
Office

506
BU
Bournemouth
University

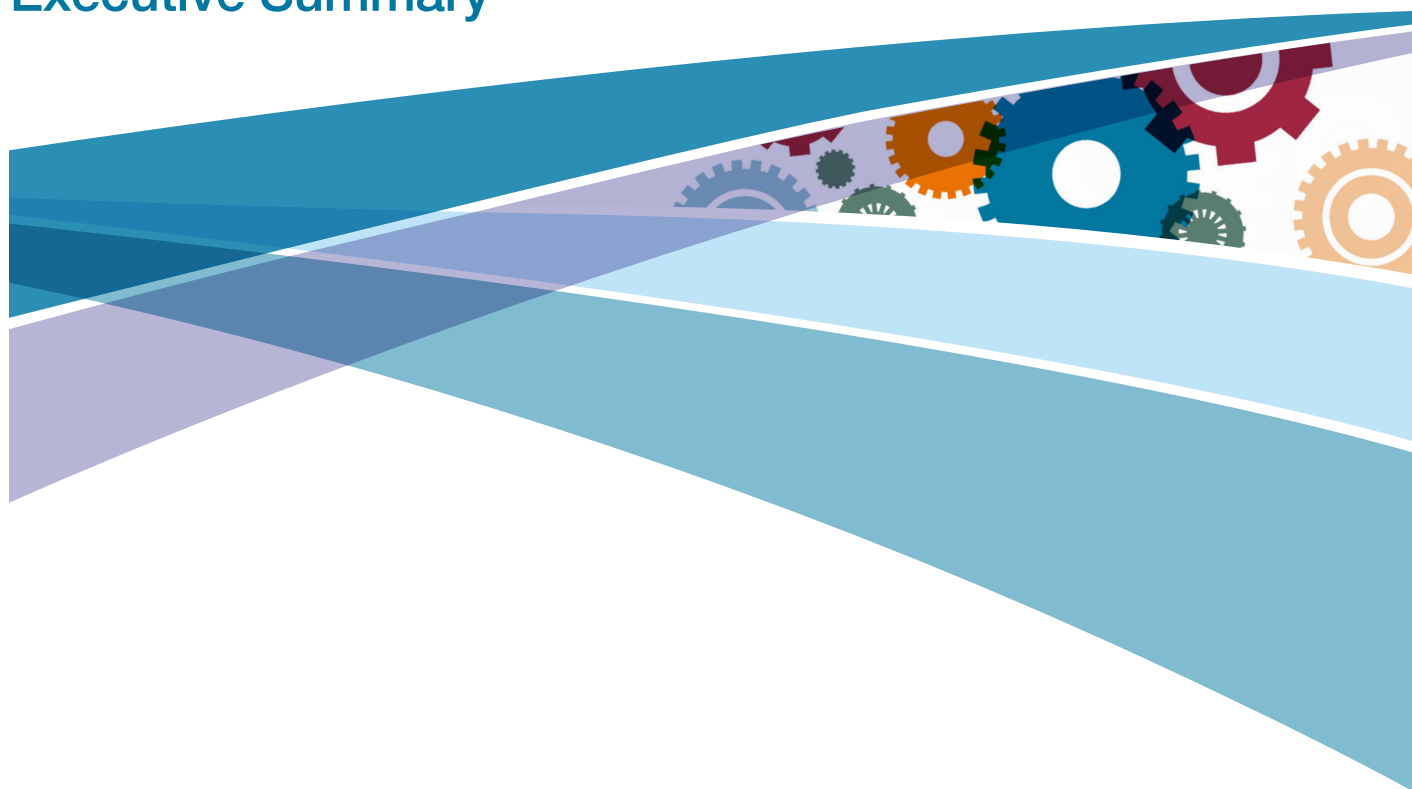
CIPPM Centre for
Intellectual Property
Policy & Management

ECONOLYST

THE 3D PRINTING & ADDITIVE
MANUFACTURING PEOPLE

A Legal and Empirical Study into the Intellectual Property Implications of 3D Printing

Executive Summary



Research commissioned by the Intellectual Property Office, and carried out by:

Dinusha Mendis, Davide Secchi and Phil Reeves

March 2015

This is an independent report commissioned by the Intellectual Property Office (IPO). Findings and opinions are those of the researchers, not necessarily the views of the IPO or the Government.

Dr. Dinusha Mendis is Associate Professor in Law and Co-Director of the Centre for Intellectual Property Policy and Management (CIPPM), Bournemouth University, UK
E-mail: dmendis@bournemouth.ac.uk

Dr. Davide Secchi is Senior Lecturer in Organisational Behaviour at Bournemouth University and from April 2015, Associate Professor in Organizational Cognition, Research Cluster for Cognition, Management, and Communication (COMAC), University of Southern Denmark, Slagelse
E-mail: dsecchi@bournemouth.ac.uk / secchi@sdu.dk

Dr. Phil Reeves is Managing Director of Econolyst Ltd, Derbyshire, UK
E-mail: phil.reeves@econolyst.co.uk

This is the third of a sequence of three reports on the intellectual property implications of 3D printing commissioned to evaluate policy options in relation to online platforms and selected business sectors.

Study I presents a legal and an empirical analysis of 3D printing online platforms; Study II offers an insight into the current status and impact of 3D printing within selected business sectors by employing a case study approach; the executive summary provides a summary of the findings of Studies I and II and provides conclusions and recommendations for Government, Intermediaries (online platforms) and Industry.

The commissioned project was led by Dr. Dinusha Mendis in collaboration with Dr. Davide Secchi and Dr. Phil Reeves.

Acknowledgements: The authors are grateful to Samreen Ashraf and Hayleigh Boshier (PhD Candidates) at Bournemouth University for their research assistance.

ISBN: 978-1-908908-85-8

A Legal and Empirical Study into the Intellectual Property Implications of 3D Printing: Executive Summary

Published by The Intellectual Property Office
 March 2015

1 2 3 4 5 6 7 8 9 10

© Crown Copyright 2015

You may re-use this information (excluding logos) free of charge in any format or medium, under the terms of the Open Government Licence. To view this licence, visit <http://www.nationalarchives.gov.uk/doc/open-government-licence/> or email: psi@nationalarchives.gsi.gov.uk

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

Any enquiries regarding this publication should be sent to:

The Intellectual Property Office
 Concept House
 Cardiff Road
 Newport
 NP10 8QQ

Tel: 0300 300 2000
 Fax: 01633 817 777

e-mail: information@ipo.gov.uk

This publication is available from our website at www.ipo.gov.uk

Introduction

In 2012, the Big Innovation Centre, in their Report ‘Three Dimensional Policy: Why Britain needs a policy framework for 3D Printing’¹ provided a number of recommendations. A key recommendation was to review the intellectual property implications of 3D printing². Whilst a number of academics^{3,4} have examined the implications for intellectual property (IP) law as a result of the recent proliferation of 3D printing, there is a lack of empirical evidence⁵ to determine whether this emerging technology will have an impact on IP laws.

At the same time, there is limited research on the impact of 3D printing on IP law in the industrial sector. The existing literature does not sufficiently indicate the extent, use and regulation of 3D printing in the replacement parts, customised goods and high-value small status goods sectors. As such, the current research provides an insight into the use, adoption and regulation of 3D printing in the selected industries whilst outlining the IP implications.

This two-part Study (represented in Studies I and II) adopts a quantitative and qualitative approach respectively to fill a gap in the research relating to 3D printing. The two Studies provide for an overarching empirical and legal analysis into the current position of 3D printing. Particularly it offers new data and findings on the exploration of online platforms dedicated to 3D printing as well as its impact in selected industries. This synopsis reports the purpose, scope, methodology and key findings from the two complementary studies carried out by the researchers.

Context: Introduction to 3D Printing

“Like the magic wand of childhood fairy tales, 3D printing offers us the promise of control over the physical world. 3D printing gives regular people powerful new tools of design and production ... In a 3D printed future world, people will make what they need, when and where they need it”⁶.

Whilst it may be some years, before Lipson and Kurman’s prediction is realised, it is true that 3D printing gives people powerful new tools of design and production. However, a 3D printer will only operate on the basis of the instructions provided from a computer in the form of well-designed electronic files. In fact, a “3D printer without an attached computer and a good design file is as useless as an iPod without music”⁷. Furthermore, the selection of materials is equally important to ensure that an object can be 3D printed.

The technology is not new. The first patent was filed in 1971 and was granted in 1977 to American Wyn Kelly Swainson⁸. Before that, an article written by David Jones on the concept of 3D printing was published in the *New Scientist* on 3 October 1974⁹. Ultimately, it was Charles Hull who led the way for the launch of the first commercial 3D printer in 1988, made possible by a patent granted in March 1986 for an ‘Apparatus for Production of Three-Dimensional Objects by Stereolithography’¹⁰.

Since then, the technology has continued to develop significantly¹¹ and around the year 2000, it was suggested that 3D printed parts could also be used directly as end-use products, eliminating the need for traditional production processes such as moulding, casting and machining¹². This direct approach to part production was initially called ‘Rapid Manufacturing’, before being standardised by the American Society for Testing and Materials as ‘Additive Manufacturing’ (AM)¹³.

However, the term AM failed to gain popularity with the media and the general public, who have tended to adopt the term 3D printing. The two terms (3D printing and AM) relate to different activities, although they are quite often used interchangeably¹⁴. Within the context of this research, Study I adopts the term 3D printing whilst Study II uses the two terms as relevant in making reference to businesses or consumers.

Purpose, Scope and Methodology

Purpose and Scope

This two-part Study provides a quantitative and qualitative insight into the IP implications arising from 3D printing, whilst examining the extent of the use of 3D printing within online platforms and selected industrial sectors.

Study I, titled 'A Legal and Empirical Study of 3D Printing Online Platforms and an Analysis of User Behaviour' provides a legal analysis (Section A), an empirical study (Section B) before providing conclusions and recommendations (Section C).

The legal analysis commences with a consideration of the copyright implications arising from the access and use of online platforms. Whilst 3D printing raises a variety of issues relating to Intellectual Property Rights (IPRs), Section A, focuses particularly on the implications for copyright laws. In particular, Section A considers the copyright implications arising from the (1) creation of an object design file; (2) modification of an existing design; and/or (3) scanning of a physical object. In exploring these scenarios, the Report attempts to answer the following questions, amongst others: can a CAD file be protected under copyright law? Does it qualify as a literary work? Can 'modified' files lead to new derivative works under copyright law?

The discussion on copyright law is followed by an overview of three online platforms (Thingiverse, 123D and GrabCad) dedicated to 3D printing – selected on the basis of being the platforms with the highest number of registered users before moving on to a consideration of the governing laws and choice of jurisdiction relating to these online platforms.

Section B provides an overview of how the online platforms operate and to do so, analyses data extracted from 17 online platforms dedicated to the sharing of 3D designs for 3D printing. Section B begins by presenting a description of the variables available in the data collected to specify operations – i.e., how the online platforms dedicated to 3D printing work. The analysis is also used to provide information on the depth of the phenomenon – i.e. qualifying the content and how it is shared. Finally, the analysis is used to define the width – i.e. the range and scope of sharing (of design files) and what seem to be its drivers. As such, the current research attempts to evaluate the extent of this phenomenon amongst users and aims to explore and understand the activities carried out on online platforms. In doing so, the research examines the price, downloads, licences, type of physical objects, which are shared and the implications for IP laws.

The analysis in Section B reflects an exploratory discussion leading to a number of conclusions. It is therefore important to point out that the researchers do not follow a classic hypothesis-testing scheme but perform the analysis aiming at finding whether relationships among variables exist and what their shape is.

Study II titled ‘The Current Status and Impact of 3D Printing within the Industrial Sector: An Analysis of Six Case Studies’ provides an insight into the current status and impact of 3D printing within the business sector by employing a case study approach.

Study II presents six case studies, each looking at a potential consequence of AM and 3D printing in various industrial sectors. The case studies are arranged into three key themes: “Replacement Parts”, “Customised Goods” and “High Value Small Status Goods” and consider the drivers and barriers for the adoption of AM technologies and the effects that technology development could have on these sectors in the future. Furthermore, Study II identifies the various implications for IP laws within the selected business sectors.

The first two case studies address issues relating to Replacement Parts and consider how AM will affect the supply of aftermarket parts to the consumer. For example, what is the likelihood of automotive manufacturers, third-party manufacturers and consumers producing spare parts for vehicles using AM technologies? What are the implications of consumers and independent repair companies being able to manufacture spare parts for domestic appliances on demand, using consumer 3D Printers? The case studies also consider how consumers are using online platforms to share digital designs and models of spare parts and its impact on the domestic appliances aftermarket.

The two case studies within the Customised Goods theme address how AM enables unique products to be manufactured that are tailored to consumers’ needs, and the IP challenges that arise therein. In particular, the case studies consider the IP implications when the consumer has an increased role in the design of products and investigates the extent to which scanning technologies will enable users to replicate and modify existing physical objects using AM and 3D printing. The technical limitations of the technology for both consumer-level and professional-level scanners are also highlighted in this section.

The final two case studies within the High Value Small Status Goods theme examine the impact that AM has on consumer products that have a low functional purpose, such as collectible figurines or sculptures. The IP implications of extracting printable data and content from sources of Computer-Generated Imagery (CGI) such as computer games are considered. Furthermore, this final case study explores how artists and designers protect their digital content from IP infringement that is enabled through commercial AM technology and home 3D printing.

Methodology

A black-letter law methodology is used for the legal analysis followed by a quantitative method for the empirical analysis in Study I. The legal research comprises of a literature-based analysis and utilises a systematic review technique to explore the various issues, which also had the benefit of providing for a high level of flexibility. In particular, the assessment of the implications for copyright law followed by the Governing Laws of online platforms and Choice of Jurisdiction aims to represent the current landscape in relation to 3D printing and IP law.

For the empirical study, data was collected from 17 websites, namely: 123D, 3DLT, CGTrader, Cubehero, Cubify, Cuboyo, GrabCad, i.Materialise, Kraftwurx, Leopoly, Ponoko, Sculpteo, Shapeways, Sketchup, the Pirate Bay, Thingiverse and Youimage. The data extracted from

these 17 online platforms was analysed to understand how these platforms operate. The analysis established that the total number of files shared on the platforms was 385,118 and the total number of users 48,715. Data was retrieved on January 2014 and covers six years, from January 2008 to January 2014. One of the shortcomings of the analysis was the lack of a clear and homogeneous standard for these websites resulting in user-related information varying significantly from website-to-website.

Study II employs a qualitative methodology. The researchers interviewed key stakeholders within selected industrial sectors to identify existing IP implications arising from 3D printing in the UK and EU. The names of individuals and / or companies are identified where possible in the course of examining the findings.

Findings and Conclusions

From the data retrieved in **Study I**, there is nothing to indicate that the activity on 3D printing online platforms is a mass phenomenon yet. As such, there is no urgency to legislate on 3D printing at present.

Whilst there is little to indicate infringement at a noticeable level in the current landscape, interest and activity is growing exponentially every year¹⁵ and conclusions can be drawn from such activities. These in turn highlight the potential for future IP issues.

- Files that carry the label ‘fashion’ attract a higher number of views and downloads while labels such as ‘art’ and ‘robot’ are marketed at higher prices;
- Files bearing the tag ‘miniature’, ‘art’, and ‘jewellery’ are more prevalent on the online communities leading to hypothesise that hobby and leisure is one of the most attractive areas for these platforms;
- The proliferation of by-products such as mobile software applications that interact with 3D printing platforms provide the tools for the modification of CAD files;
- Higher views and downloads are also dependant on (a) the choice of the platform and (b) the type of brand/product. A typical example is the iPhone-labelled files, which attract more downloads and views. This is a paradigmatic example of what can be achieved with the instrumental use of a popular brand/product. The more popular a product the more likely it is that people would look for something to complement it (e.g., a case, a decorative stand);
- It is interesting to note that the number of downloads is unrelated to the price. This could be due to a lack of accessibility to the relevant materials or lack of access to more sophisticated 3D printers; i.e., those that are capable of printing more expensive files.

Online platforms should explain different licence types to users and assign the most appropriate licence as a default with ‘opt-out’ being an option. This is because the vast majority of people

(65%) who use these online platforms do not license their work. The minority 35% that do license their work make their choice in accordance with the product they are uploading.

There should be clarity in relation to CAD files particularly in relation to their copyright status. Any future regulation efforts should therefore be focused on providing guidance on the access and use of CAD files.

Study II suggests that there will be little commercial impact on either the automotive or domestic appliance aftermarket within the next decade as a function of either consumer 3D printing or industrial AM.

The current technology does not lend itself to printing parts that are of a suitable quality to replicate traditionally manufactured automotive or domestic appliance components. Furthermore, the economics of AM production are of a greater magnitude than the accepted price point of current spare parts. However, as the technology continues to grow, steps should be taken in relation to traceability of spare parts, particularly in the car spare parts sector.

If hardware and software reach a point where a product can be printed easily and quickly and it will work in the appliance or automotive industries without having to modify the part through iteration, a wider consumer base may adopt the technology.

There is evidence that consumer orientated software tools will develop significantly in the coming years, through increased awareness by software vendors relating to design and personalisation demands. Consequently, the technical skill level of consumers will develop along with an increase in creativity driven through the resurgence of making 3D printed products within the home and community.

Over time industrial additive manufacturing will reduce in price, which will open the market for more affordable products. On the other hand, the capability of home 3D printing technologies will remain limited for the foreseeable future, as they lack the accuracy, scale and ability to produce truly robust parts to make desirable consumer or automotive products.

The technology relating to consumer-level 3D scanning is currently limited and will remain so for the foreseeable future with little risk to businesses and IP laws. Steps should however be taken to consider developing legitimate channels through which businesses can provide consumers with access to legal downloads of their products for 3D printing.

Key Recommendations

For Government

A premature call for legislative and judicial action in the realm of 3D printing could stifle the public interest of “fostering creativity and innovation and the right of manufacturers and content creators to protect their livelihoods”¹⁶. However, as 3D printing continues to grow, it is important to address the intellectual property issues arising in this area. As such, it will be prudent to take

steps to cultivate a climate better suited to tackle impending IP issues more successfully and in a manner, which takes into account the interests of all stakeholders.

There needs to be clearer guidance on defining whether a CAD file is capable of copyright protection. The territorial nature of copyright law, coupled with the exterritorial nature of online platforms and CAD files shared therein could lead to uncertainty and complex issues in the future.

It is recommended that the UK Intellectual Property Office (UKIPO) establish a Working Group to cover the various IP rights which may need to be tackled in the future. The Working Group should also provide clarity on the status of CAD files and how they can best be used in industry. The Group should also consider how best to tackle the traceability of 3D printed spare parts.

For Intermediaries (Online Platforms)

As mentioned above, 65% of users engaged in the activities of 3D printing on online platforms do not license their work, leaving their creations vulnerable and open to infringement whilst losing the ability to claim authorship.

It is recommended that online platforms provide more awareness and understanding of the different types of licences. This can be achieved by explaining the nuances relating to each licence in clear and simple language, rather than simply 'encouraging' the user to adopt a particular type of licence. Furthermore, online platforms can assign the most appropriate licence as a default with 'opt-out' as an option.

Online platforms increasingly offer tools for the creation, modification, and transformation of object-designed files. For example, these include, 123D Sculpt, Meshmixer, Tinkercad, Workbench and MakerBotDigitizer¹⁷ amongst many others. As online platforms and user-numbers continue to grow it is recommended that spin-offs and by-products offered by the online platforms be monitored.

For Industry

One recommendation for industry would be to adopt secure streaming of 3D CAD files via an Application Programming Interface (API) thereby embracing a 'pay-per-print' business model¹⁸. This is already in operation amongst companies such as Authentise¹⁹, Secure3D²⁰, ToyFabb²¹. This business model removes the need for a CAD file to be sent to the consumer²²; instead the build instructions are sent directly to the printer, which, in turn, prints out the number of objects that have been purchased. This can be particularly effective for the customised goods industry.

Manufacturers could also consider licensing CAD files more widely, thereby opening up doors to a range of outlets selling 3D CAD files. This will avoid locking the manufacturer into an agreement through a system such as a 'one-stop-shop' for (spare) parts. Although a one-stop-shop may take away the costs of manufacture, transportation and storage whilst reducing potential infringement of IP laws, it can lead to a monopoly-situation, which should be avoided.

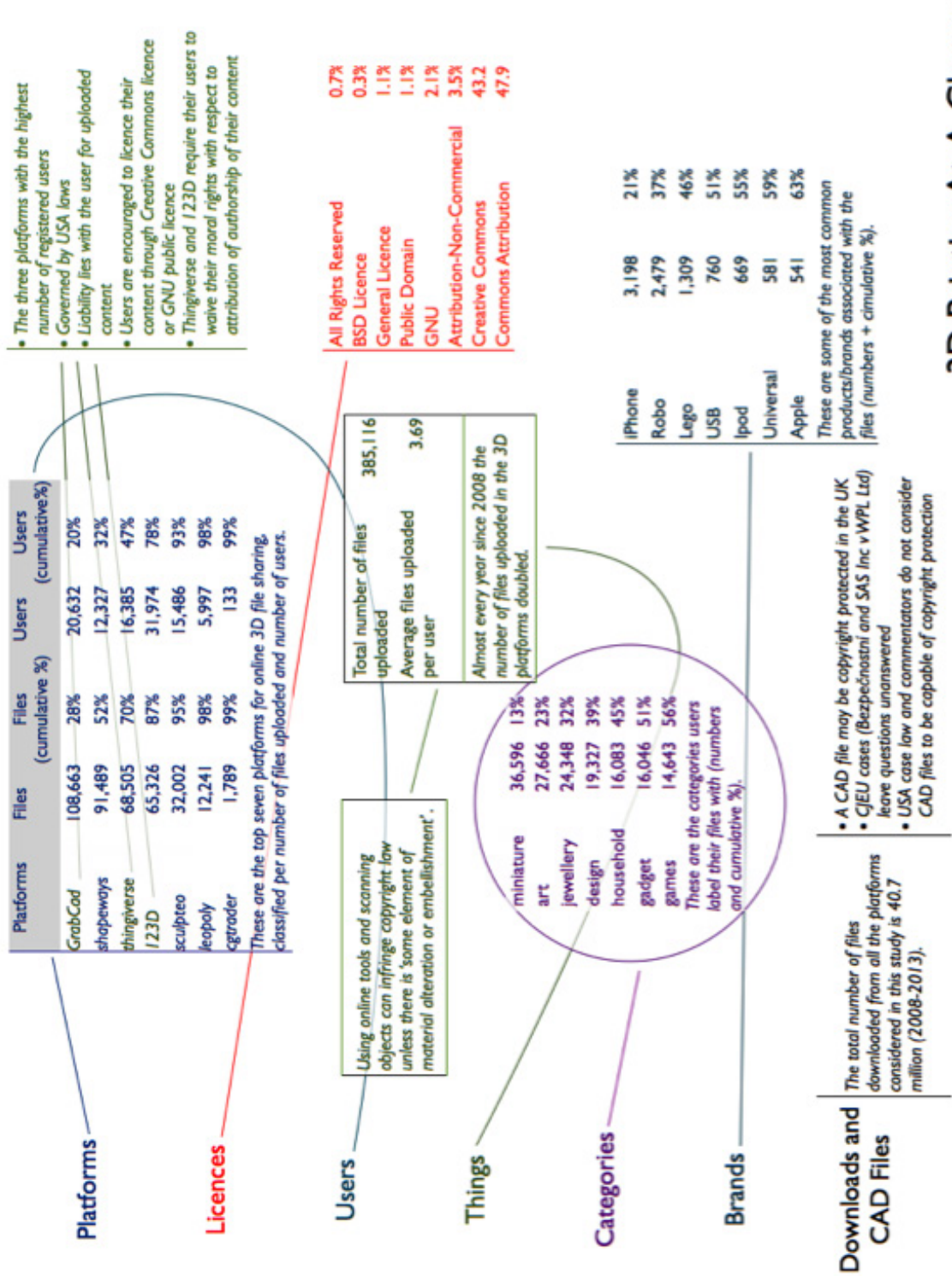
It is recommended that the automotive industry give consideration to the traceability of 3D printed spare parts, particularly in relation to the safety and usability of the spare part.

Conclusion

The present research and the accompanying data concludes that taking into account accessibility to materials, sophisticated printing machines, costs and economics for the average user, the impact of this technology will not be felt among the general public for a few years to come. Although it is too early to tell when this will happen, the researchers conclude that a technological breakthrough is needed to make 3D printing an everyday reality.

- 1 Sissons A., & Spencer T., Three Dimensional Policy: Why Britain needs a policy framework for 3D Printing' (Big Innovation Centre; October 2012) Available at http://biginnovationcentre.com/Assets/Docs/Reports/3D%20printing%20paper_FINAL_15%20Oct.pdf
 - 2 Ibid., see p. 33. See also, Intellectual Property Office, 3D Printing: A Patent Overview (Newport: Intellectual Property Office; November 2013), p. 10. Available at <http://www.ipo.gov.uk/informatics-3d-printing.pdf>
 - 3 Bradshaw S., Bowyer A., & Haufe P., The Intellectual Property Implications of Low-Cost 3D Printing (April 2010) Vol. 7, Issue 1 Script-ed pp. 1-31; Mendis D., Clone Wars: Episode I – The Rise of 3D Printing and its Implications for Intellectual Property Law: Learning Lessons from the Past? [2013] 35(3) European Intellectual Property Law pp. 155-169; Mendis D., 3D Printing Enters the Fast Lane [2014] Intellectual Property Magazine, pp. 39-40; Mendis D., Clone Wars: Episode II – The Next Generation: The Copyright Implications relating to 3D Printing and Computer-Aided Design (CAD) Files [2014] 6(2) Law, Innovation and Technology pp. 265-280; Li P., Mellor S., Griffin J., Waelde C., Hao L., & Everson R., Intellectual Property and 3D Printing: A Case Study on 3D Chocolate Printing [2014] 2 Journal of Intellectual Property Law and Practice, pp. 1-11.
 - 4 Weinberg M., What's the Deal with Copyright and 3D Printing (2013) available at <https://www.publicknowledge.org/news-blog/blogs/whats-the-deal-with-copyright-and-3d-printing>; Weinberg M., It Will be Awesome If They Don't Screw It Up: 3D Printing, Intellectual Property and the Fight Over the Next Great Disruptive Technology (2010) available at <https://www.publicknowledge.org/news-blog/blogs/it-will-be-awesome-if-they-dont-screw-it-up-3d-printing> ; Simon M., When Copyright Can Kill: How 3D Printers Are Breaking the Barriers Between Intellectual Property and the Physical World (Spring 2013) 3(1) Pace. Intell. Prop. Sports and Entertainment Law Forum pp. 59-97. Available at <http://digitalcommons.pace.edu/pipself/vol3/iss1/4> ; Susson M., Watch the World "Burn": Copyright, Micropatent and the Emergence of 3D Printing [January 2013] Chapman University School of Law, Available at http://works.bepress.com/matthew_susson/3 ; Rideout B., Printing the Impossible Triangle: The Copyright Implications of Three-Dimensional Printing (2011) 5(1) Journal of Business Entrepreneurship & Law pp. 161-180. Available at <http://digitalcommons.pepperdine.edu/jbel/vol5/iss1/6> ; Santoso S. M., Horne B. D., & Wicker S. B., Destroying by Creating: Exploring the Creative Destruction of 3D Printing Through Intellectual Property(2013). Available at http://www.truststc.org/education/reu/13/Papers/HorneB_Paper.pdf
 - 5 Moilanen J., Daly A., Lobato R., & Allen A., Cultures of sharing in 3D Printing: what can we learn from the license choices of Thingiverse user? (May 21, 2014) Journal of Peer Production, Forthcoming, Available at SSRN <http://ssrn.com/abstract=2440027>
 - 6 Lipson H., & Kurman M., Fabricated: The New World of 3D Printing (Indiana: John Wiley & Sons, Inc.; 2013), pp. 11.
 - 7 Lipson H., & Kurman M., Fabricated: The New World of 3D Printing (Indiana: John Wiley & Sons, Inc.; 2013), p. 12.
 - 8 Application no. 05/165042 filed 23 July 1971. U.S. Patent 4,041,476 'Method, medium and apparatus for producing three-dimensional figure product' granted 9 August 1977.
-

- 9 Jones D., 'Ariadne' Column, 3 October 1974, New Scientist, p. 80.
 - 10 Application no. 06/638,905 filed 8 August 1984. U.S. Patent 4,575,330 'Apparatus for Production of Three-Dimensional Objects by Stereolithography' granted 11 March 1986.
 - 11 Rowe Price T., A Brief History of 3D Printing: From 1980's to 2010 [2011] Available at http://individual.troweprice.com/staticFiles/Retail/Shared/PDFs/3D_Printing_Infographic_FINAL.pdf See also, Gartner's Hype Cycle for Emerging Technologies [2014] Available at <http://www.gartner.com/newsroom/id/2819918>
 - 12 Hague R. & Reeves P., Additive Manufacturing and 3D Printing [June 2013] Issue 55, Ingenia pp. 38-45 at p. 39.
 - 13 Hague R., & Reeves P., supra n. 15 pp. 39-40.
 - 14 Additive Manufacturing refers to the production of end-use layer manufactured parts produced within a business-to-consumer supply chain. 3D Printing is used to refer to the manufacture of layer-manufactured products within the home or community.
 - 15 Lipson H., & Kurman M., Fabricated: The New World of 3D Printing (Indiana: John Wiley & Sons, Inc.; 2013); Hoskins S, 3D Printing for Artists, Designers and Makers (London: Bloomsbury; 2013); Anderson C., Makers: The New Industrial Revolution (New York, London: Random House; 2012).
 - 16 Susson M., Watch the World "Burn": Copyright, Micropatent and the Emergence of 3D Printing [January 2013] Chapman University School of Law, Available at http://works.bepress.com/matthew_susson/3 at p. 39.
 - 17 See all apps and their functions at <http://www.123dapp.com/create>
 - 18 See Authentise's API at <http://www.authentise.com/api>
 - 19 Authentise at <http://www.authentise.com>
 - 20 Secure3D at <http://secured3d.com>
 - 21 ToyFabb at <http://www.toyfabb.com>
 - 22 However, companies such as ToyFabb allow for both options: Customers can either buy the 3D design file as an STL file or it can be streamed directly to the customers' 3D printer. See, <http://www.toyfabb.com/get-creative>
-



3D Printing At-A-Glance

Concept House
Cardiff Road
Newport
NP10 8QQ

Tel: 0300 300 2000
Fax: 01633 817 777

For copies in alternative formats please
contact our Information Centre.

**When you no longer need this booklet,
please recycle it.**

DPS/IP Research-03/15



CUSTOMER
SERVICE
EXCELLENCE



Seven Best Practices for Fighting Counterfeit Sales Online

Executive Summary

Counterfeit sales represent seven percent of all global trade.¹ The damage these sales do to rightful brand owners goes well beyond revenues and profits: Numerous reports have suggested that counterfeit and piracy trade supports terrorism, organized crime and other threats to both national security and human rights. The Internet's rapid growth — along with its instant global reach and anonymity — has significantly escalated the situation.

An entire online supply chain, parallel to legitimate distribution channels, has flourished around counterfeit goods. Online B2B marketplaces, in addition to e-commerce sites — many promoted via social media and search engines — commonly traffic in counterfeit goods. Fake products acquired on wholesale sites are sold across multiple digital channels, or at flea markets and shops in the physical world.

Deceptive use of proven marketing techniques — paid search ads, search engine optimization, email and social media campaigns, branded domain names and more — are important parts of this illicit ecosystem, as savvy counterfeiters apply marketing best practices.

Fortunately, brand owners can adopt their own proven best practices to successfully combat online counterfeit sales. Unlike anti-counterfeiting strategies in the physical world, however, a two-pronged approach is necessary: Brand owners must choke off counterfeit sales at both promotional and distribution points. Technology exists for identifying and quantifying worldwide online counterfeiting activity in both promotional and distribution channels, and, once visible, infringement can be prioritized and attacked. The battle against online counterfeit sales can be won. With billions in revenues, critical customer loyalty and even public safety and human rights at stake, it must.

Contents

Counterfeiting: A Growing Online Threat 3

Counterfeiting’s Real Cost to Business 3

How Counterfeiting Thrives Online 4

Beating Back Counterfeiters Online: Seven Best Practices 5

Conclusion: The Fight Is Yours to Win 9

Counterfeiting: A Growing Online Threat

“If you can make it, you can fake it.” Unfortunately, the old saying is all too true. Sales of counterfeit goods affect a wide range of industries, from high-margin luxury and technology goods to low-margin consumer goods like batteries, shampoo, gasoline and food.

The problem is growing, in part because the volume of fake goods produced is rapidly increasing — especially in countries like China, where manufacturing capacities continue to skyrocket. Mainland China was the point of origination for approximately \$1.2 billion of the \$1.7 billion in counterfeit goods confiscated by U.S. law enforcement agencies in 2013.²

This growth in supply helps fuel the exploding demand — especially online. The Internet’s rapid growth — along with its instant global reach and anonymity — has significantly escalated the situation, moving the sale of counterfeit goods from the local street corner to a global marketplace. Because criminals can quickly and easily set up e-commerce storefronts or place listings on B2B marketplaces cost-effectively, their activities will continue to cost legitimate businesses billions in lost revenue.

Counterfeiting’s Real Cost to Business

According to the secretary general of the ICC, multinational manufacturers lose roughly ten percent of their top-line revenue to counterfeiters — but the impacts go well beyond the revenue hit. For some companies, perceived brand value suffers when knock-offs become plentiful. Brands may even lose representation in distribution channels when resellers and affiliates see a reduction in demand due to competition from fakes. Additionally, the availability of cheaper, albeit fake, alternatives can exert downward pressure on legitimate brand pricing.

Other impacts include product safety issues — especially in pharmaceutical, automotive, aviation, healthcare, electronics and similar industries — accompanied by increased legal liability risks. And as consumers experience quality problems with fake goods, the legitimate brand’s customer service and warranty costs can climb.

Marketing costs also rise as illicit sellers bid up paid search advertising costs and erode legitimate search engine optimization (SEO) investments. Finally, as more customers encounter inauthentic brand experiences, both loyalty and lifetime customer value suffer.

How Counterfeiting Thrives Online

Counterfeits in Digital Channels Affect Multiple Industries:

Tablets

Listings for clones, suspected counterfeits or gray market tablet computers numbered more than 23,000 in a single day

More than 6,600 cybersquatted sites taking advantage of tablet brands generated more than 75 million annual visits

Luxury Goods

Suspected counterfeiters attracted 120 million annual visits to their e-commerce sites, representing almost half the traffic generated by the legitimate dot com sites for five luxury brands

Brandjackers set up more than 1,100 cybersquatted sites touting luxury brands and more than 50 suspicious vendors purchased luxury brands keywords in paid search scams

Sports Apparel

Suspected counterfeiters attracted 56 million annual visits to e-commerce sites annually

Suspected counterfeiters sold almost 1.2 million suspicious jerseys via e-commerce and business-to-business (B2B) marketplaces sites annually

We found more than 6,000 suspects selling more than 1.2 million shirts or jerseys annually over the Internet, generating nearly \$25 million in revenue.

Source: MarkMonitor Brandjacking Index®

An entire online supply chain — parallel to legitimate distribution channels — has grown around counterfeit goods. This illicit but highly profitable industry takes advantage of the same online tools, techniques and best practices employed by legitimate brands online.

The contrasts with counterfeiting in the physical world are important to understand, and are based upon the Internet's global reach, anonymity and efficiency. These attributes — and especially the digital world's powerful promotional potential — have enabled online counterfeiters to dramatically (and rapidly) outstrip all the street corner fakes, flea markets and "Canal Street districts" that exist.

In the wholesale trade, B2B marketplaces (also known as trade boards) often traffic in counterfeit goods. At the retail level, counterfeiters also use marketplaces to supply counterfeit goods to consumers. It's not unusual for counterfeiters to acquire fake goods on wholesale sites, only to resell them to consumers via digital channels — in addition to offline flea markets, bazaars and even retail shops.

Promotion is an important part of this illicit ecosystem. Counterfeiters use the same tactics as legitimate marketers, such as paid search

ads and search engine optimization to lure buyers to their sites. According to Direct Magazine, fully 14 percent of searches on a branded item lead online users somewhere other than the legitimate brand's site. While some of these searches may lead to legitimate resellers or partners, it's reasonable to assume that many of them end up on the site of a counterfeiter.

Some counterfeit sellers also employ unsolicited email — spam — to boost their site traffic. This is especially prevalent among sellers of fake pharmaceuticals, software and luxury goods such as watches, jewelry and high-end apparel. They also make use of cybersquatting techniques, using branded terms in domain names in order to attract Web traffic and convey authenticity. And, as savvy marketers, they take advantage of inbound linking strategies and other SEO techniques to sell their illicit goods online.

The counterfeiting ecosystem extends to popular auction and exchange sites where direct searches frequently include counterfeit goods among their results. Links to sites pushing counterfeit wares can also be found on social media venues such as social networking sites, blogs and micro-blogs.

Clearly, legitimate and counterfeit ecosystems overlap — with some auction and e-commerce sites selling both real and fake goods — and this makes the problem more difficult to address. There are best practices, however, which can help brands minimize the damage from counterfeit sales in digital channels.

Beating Back Counterfeiters Online: Seven Best Practices

While the sale of counterfeit goods in the physical world is a timeworn tradition — if an unwelcome one — the online counterfeiting ecosystem offers unique challenges that require a unique approach. Proven best practices have emerged from brands that have actively and successfully engaged in combating counterfeit sales online.

1. Attain global visibility. Before a brand can understand the scope of the threat posed by online counterfeit sales, it must expose and quantify the problem. Counterfeiters operate over a wide array of online channels; all of these, including online marketplaces, e-commerce sites, message boards and the rest, must be monitored and analyzed. There's some good news for brands, however. Our experience shows that ten online marketplaces account for fully 80 percent of all marketplace traffic. Monitor these marketplaces, and you're watching a significant share of traffic.

Counterfeiters depend on technology to drive sales volumes so approach the monitoring challenge with the same tools and leverage technology to form a complete and accurate picture of the counterfeiting challenge that your brand faces.

2. Monitor points of promotion. While it's obviously important to identify and shut down distribution channels, it's almost certain that counterfeiters will regularly seek new sales venues. So it's just as critical to monitor the online promotional channels used by these criminals.

Counterfeiters use the same effective promotion techniques employed by legitimate marketers while leveraging the powerful, highly recognizable brands built by experts. Using paid search advertising, links within social media, black hat SEO tactics, cybersquatting and spam, they successfully steer traffic to their illicit offerings, and diminish the marketing ROI of legitimate brands. Monitoring for these promotional efforts is critical — and enables our next best practice.

3. Take proactive action. Counterfeiters obviously encounter more success when left to operate unchallenged; they're also known to shift their energies to more passive targets when brands visibly fight back. Once a brand understands where

the greatest threats lie, aggressive action is the best strategy. Brands should:

- **Set priorities.** Identify the biggest offenders, offering the greatest number of counterfeit goods in the most highly trafficked venues, and address them first. Brand owners should determine which counterfeit goods are generating the largest sales, and target them first as well.
- **Watch for cybersquatters.** Brands should actively monitor the Internet for unauthorized use of their branded terms in domain names. This will aid in rapid detection of e-commerce sites selling counterfeit or unauthorized goods — and frequently also uncovers other abuses such as false association with offensive content like pornography.
- **Become a difficult target.** Brands that visibly, vigorously fight to remove counterfeit goods from online venues often see a dramatic drop in infringement against their brands.
- **Use all your weapons.** Most online channels provide mechanisms for dealing

with counterfeit sales situations. Online marketplaces, for example, typically have policies and procedures enabling brand owners to report listings that infringe their brand.

Search engines offer similar facilities. Major search engines have procedures for requesting the removal of ads linked to counterfeit sites. Websites can also be removed from search results pages if they are found to violate copyright laws (a common practice among sites selling counterfeits, typically through unauthorized use of product images).

- **Get help from friends.** Industry relationships can be powerful weapons in the fight against online counterfeiting. When choosing a brand protection solution provider, look for one with established ties with thousands

of ISPs and Registrars worldwide. Simply put, these ties make it possible to get counterfeit sites shut down more quickly—thereby minimizing brand owner losses. Trade associations such as the International AntiCounterfeiting Coalition (IACC), the Anti-Counterfeiting Group (ACG) and the American Apparel and Footwear Association (AAFA) also provide resources and advice on best practices for fighting counterfeiters.

4. Fight online counterfeit sales holistically. Online counterfeit sales are easier to address when the entire enterprise participates. That means brand owners should set up a cross-functional task force to address the issue in a coordinated, holistic manner.

Stakeholders — and, therefore, recommended participants — will vary by industry and enterprise, but can include legal, marketing, risk management, loss prevention,

The Best Tools for Fighting Technology-enabled Counterfeit Sales

Brand:	Snap-on
Challenge:	Significant online sales of counterfeit Snap-on tools, resulted in erosion of revenues, perceived brand value and customer loyalty.
Response:	Snap-on employed sophisticated monitoring and detection technology solutions to fight online counterfeit sales.
Results:	Counterfeit products valued at \$1.2 million — found in 4,900 illegal auction listings — were identified and removed in coordination with an online auction site.

channel sales management, manufacturing, supply chain management and other functional units.

Because fighting online counterfeiting requires attacking both promotional and distribution channels, this group needs to address more facets of the problem than seen in the physical world. All of these groups can, and should, set priorities and strategies for detecting, reporting and responding to infringers and should continue to inform the process as their situations and perceptions dictate.

5. Let online intelligence inform offline defense measures. Because offline measures — physical investigations, factory raids and other activities — can be costly and time-consuming, it's critical to know where they should be focused. Online intelligence can help identify the most egregious infringers, so that offline defensive efforts can be focused where they'll be most effective.

6. Act swiftly — and globally. Perhaps even more than it affects legitimate business, the proliferation of international trade offers tremendous benefits to online counterfeiters. While a domestic seller or manufacturer may seem like an easy first target, brands have learned that it's more effective to launch global anti-counterfeiting initiatives — and to get them underway expeditiously.

Prepare by ensuring your trademarks are registered internationally — especially in China, which observes a “first-to-file” policy that grants registration to whoever files first, even if it's not the true brand owner.

A global effort doesn't preclude addressing markets that target a specific country exclusively. In some cases, this will require competent language translation resources for monitoring, detection and enforcement. Most companies rely on third-party brand protection solution providers for this kind of expertise.

7. Educate your customers. Your customers can be an important ally in minimizing sales of counterfeit goods with all its associated costs. Educate your customers about the risks of buying from unauthorized sources, and recruit them to join in the effort by reporting suspicious goods and sellers. The Authenticity Foundation and its consumer site, dontbuyfakes.com, have useful resources for consumer education. Also, many brands provide form or email-based mechanisms for reporting suspected infringement. When offering such tools, be sure to reinforce the benefits of buying authentic goods from authorized sellers.

Footwear Manufacturer Stomps Online Counterfeiters

Global footwear leader Deckers Outdoor, faced with millions in online sales of counterfeit and grey market goods, moved promptly to protect its customers and its bottom line. Leveraging brand protection technology, the company was able to:

- Pinpoint — and remove or de-list — \$4.35 million in illegitimate goods and knock-offs within just 90 days
- Significantly curtail counterfeiting activity that undermined its revenues
- Enhance its brand reputation and increase customer trust and loyalty by automating and extending online enforcement

Online Intelligence Helps Focus Physical Efforts

Acushnet Company, a leader in the golf industry, leveraged online intelligence to guide a major raid in the U.K., shutting down a large counterfeiting operation that fed online distribution channels.³

Conclusion: The Fight Is Yours to Win

Online counterfeiting can heavily impact any company, affecting revenues, channel relationships, customer experience, marketing effectiveness, legal liability and more. Ignoring it — or just hoping for the best — simply isn't good business.

Fortunately, taking action can be fairly straightforward. Implementing the best practices discussed here doesn't have to involve complex organizational changes or extensive hiring efforts, as third-party solution providers can help make the effort efficient and supplement internal teams.

Global Imaging Giant Protects its Image — and Profits

Print technology leader Epson created a centralized mechanism for globally monitoring for online brand abuses including counterfeit sales.

By forming a global, cross-functional team, Epson achieved a three-fold reduction in counterfeit sales activities on consumer and B2B marketplaces. Their visible, aggressive strategy has also served to deter abuse.

To successfully reduce the negative effects of counterfeiting, many companies have found that a cross-functional team contributes a great deal to an aggressive, global anti-counterfeiting initiative.

Most importantly: To effectively choke off counterfeit sales, the strategy must focus on both distribution and promotional channels for counterfeit goods. The returns — in revenues, profits, and long-term brand value — will certainly make the effort worthwhile.

Tall Order: Fighting Counterfeiting in China

One of the most important centers of counterfeit trade is China. In addition to originating roughly \$1.2 billion of the \$1.7 billion in counterfeit goods confiscated by U.S. law enforcement agencies in 2013, China hosts vast internal marketplaces — both online and off — where counterfeit goods are traded.⁴

¹ Quintanilla, Carl. "War on Counterfeit Goods." CNBC. N.p., n.d. Web. 14 June 2013.

² United Nations Office on Drugs and Crime. "Transnational Organized Crime: Let's Put Them Out of Business." Counterfeit Goods: A Bargain or a Costly Mistake? N.p., n.d. Web. 29 May 2014.

³ CNN. "Fake Golf Clubs Scam 'Duped' eBay Customers." CNN. N.p., n.d. Web. 23 September 2009.

⁴ United Nations Office on Drugs and Crime. "Transnational Organized Crime: Let's Put Them Out of Business."

About MarkMonitor

MarkMonitor®, the world leader in enterprise brand protection and a Thomson Reuters Intellectual Property & Science business, provides advanced technology and expertise that protects the revenues and reputations of the world's leading brands. In the digital world, brands face new risks due to the Web's anonymity, global reach and shifting consumption patterns for digital content, goods and services. Customers choose MarkMonitor for its unique combination of industry-leading expertise, advanced technology and extensive industry relationships to preserve their marketing investments, revenues and customer trust.

To learn more about MarkMonitor, our solutions and services, please visit www.markmonitor.com or call us at **1-800-745-9229**.

[Boise](#) | [San Francisco](#) | [Washington, D.C.](#) | [London](#)

© 2016 MarkMonitor Inc. All rights reserved. MarkMonitor® and Brandjacking Index® are registered trademarks of MarkMonitor Inc., part of the Intellectual Property & Science business of Thomson Reuters. All other trademarks included herein are the property of their respective owners. Source Code: WPFC08042014

More than half the Fortune 100 trust MarkMonitor to protect their brands online.

See what we can do for you.

MarkMonitor Inc.

U.S. (800) 745-9229

Europe +44 (0) 207 433 4000

www.markmonitor.com

MarkMonitor®
PART OF THOMSON REUTERS

Textile counterfeiting DNA to improve supply chain integrity

September 18, 2015 / [Anna Stec](#), [James Hayward](#), [John Sherman](#), [MeiLin Wan](#)



In an era of false profits, it is incumbent on every manufacturer of consumer-facing products to ensure that their supply chain is intact and honest. Counterfeits sometime share no common content with their originals—original models that are marketed by those companies who worked (and spent) hard to establish their markets and deliver honest claims.

Other times, however, profiteers damage markets and consumers by simply diluting the original product whose claims they steal. This is a known practice to counterfeiters of pharmaceuticals, spirits, coffee—and textiles. It is a practice that affects virtually every commodity in which high- and low-priced species comprise the market, and in which quality is governed by cost of goods.

The scope of the problem

Counterfeiting is such a common practice that in some industries it is considered a rite of passage. Your brand simply has not arrived if it has not been copied. The International Chamber of Commerce estimates the “counterfeit economy” to exceed \$1.7 trillion this year. Textiles appear to dominate the shadow world with 50 percent of all illicit goods seized by U.S. Customs and Border Patrol classified as counterfeit textiles and apparel, according to Frontier Economics. A market survey by Applied DNA Sciences showed that 89 percent of cotton sheets and pillowcases were non-compliant with their label claims.

The results of counterfeiting—degraded or dangerous consumer product; financial, reputational and liability damage to companies—are the symptoms of a supply chain out of control. Beyond damaged markets, companies and consumers are becoming vulnerable to serious risk of morbidity: textiles and textile dyes that are polluted, even with carcinogenic substances. In our opinion, California’s new Transparency in Supply Chains Act signals a new wave of liability and ethical questions surrounding the health and safety of workers worldwide, including issues of slavery and human trafficking in the textile industry.

The textiles and apparel supply chains, extending right up through finished goods, are rife with product that does not match its label or documentation. Wool, cotton, synthetics and specialty fabrics are all impacted. To the consumer, counterfeits are hard to detect when a label identifies a quality fabric, which, in fact, does not contain that fabric or contains a diluted version. In clothing, footwear, sheeting, uniforms and protective wear, consumers are in increasing danger of getting far less than what they think they purchased.

Meanwhile, retailers and brand-owners can be exposed to enforcement risks from the Textile Act, enforced by the Federal Trade Commission, and the Lehman Act, which prevents competing by use of false claims and is enforced by the Department of Justice.

Controlling the supply chain:

Making the decision to control a company's textile supply chain is a true 21st-century issue, and an urgent one that needs addressing not only by the retail brands, but the entire supply chain must take responsibility for their "link" in it. This is not an easy problem to solve and it takes collaboration to pinpoint the gaps and mutually agree to close them. Two major issues are fiber substitution and origin laundering.

Fiber substitution

Long before textiles reach the consumer in the form of finished goods, the root of the problem may be traced far "upstream," starting with raw fiber or unprocessed spun yarn (greige goods), which may be "blended" but labeled as 100 percent Pima cotton, for example.

The problem of blending, or fiber substitution, is particularly acute with upscale fibers such as cashmere, merino wool and luxury cotton such as American Pima and Egyptian Giza. Too often, when a luxury fiber is sent abroad for manufacture of sheeting, towels, or apparel, the original fiber content is blended with other lower quality fiber, reducing costs and falsely improving profits for the cheater—and inevitably producing lower product quality.

Driven by the goal to maximize profits, some yarn suppliers, spinners and even fabric manufacturers may presume that their fabrics will not be subjected to testing, and, therefore, the deception for the perpetrator continues with little or no enforcement.

Origin laundering

A different form of textile identity fraud, but just as pernicious, has been called "origin laundering." In this case, the point of origin of textiles or apparel is hidden, or simply whitewashed by trans-shipping through a midpoint. One outcome, much in the news now, is the potential to undermine free-trade agreements between the U.S. and countries worldwide. Another is the ability to circumvent fair trade, sustainability requirements, human trafficking and other agreements, or other labeling based on specifying a point of origin.

Potential losses for companies extend to market share, brand reputation, stolen IP, liability to recall, potential legal and accounting costs and even criminal action. Even quality growers and manufacturers, whose every interest is in shipping pure product, share in these risks and losses, having partially lost control of their supply chains.

Reputational and market competitive issues may taint an entire segment of an industry, or even of an entire nation. And loss of market share inevitably means loss of jobs.

Furthermore, in the case of specialty fabrics, health and safety may be at risk, even as a matter of life and death. Counterfeit flame-retardant material may be defective, with obvious dire consequences. Fabric coatings, which are designed to block dangerous UV radiation on clothing, canopies, tents and other materials, are widely counterfeited, again with obvious health consequences.

The bottom line: in all cases, cheating through mislabeling or false documentation is a form of theft and, ultimately, a crime. By recapturing control over the supply chain, it's a crime that can be prevented.

A fiber to finish solution

Anxiety about supply chain lapses, and mislabeling of product is prompting some retailers to step up their use of technologies, initially through genotyping, as a supply chain diagnostic, then applying a unique botanical DNA marker, authenticated at each stage throughout the supply chain, in order to close the loop on supply chain lapses.

The results of instigating this type of technology include:

1. Quality control by verifiable authentication at each stage of the supply chain
2. Traceability with a bird's-eye view, in real time, offering a holistic transparency in the chain of custody transfer
3. Brand protection with court-defendable evidence for internal and external investigations
4. Results that have measurable benefits

Driven by the need to help supply chain managers and brand owners with solutions to help with traceability, authenticity and quality, Applied DNA Sciences developed a botanical DNA-based platform, offering a proven forensic solution that stands up to the harshest textile treatments and coatings, and is admissible as forensic evidence in court.

Fully customizable, the botanical DNA platform offers three core solutions for textiles and apparel applications:

1. fiberTyping®, a test of native cotton fiber only, it gives a clear result that determines whether the original cotton DNA is present in the fiber, yarn or fabric. Specifically, it is a patented DNA test that provides a means to verify original Extra Long Staple (*G. barbadense*) fiber cotton content, from raw fiber to greige to finished goods.
2. SigNature® T, a unique forensic identity marker that remains present from fiber stage through finished garment on a retail hanger and beyond. Applicable to any natural or synthetic fiber, yarn, fabric, or finished goods, these markers cannot be copied or simulated.
3. SigNify®, DNA authentication of the SigNature T mark at each stage throughout the supply chain. This provides forensic proof of origination and allows brands to back up their label claims to the end consumer.

This patented system enables retailers and brands to protect their products from the fiber all the way to finished goods. In this way, every one in the supply chain can be sure that their products are fully source verified, preserving the quality, integrity of premium textile goods.

This provides the necessary product claims substantiation consistent with corporate Quality Assurance and Compliance policies, as well as U.S. labeling and consumer protection laws. Brands and products can be protected, which means that products can meet consumers' expectations.

John Sherman is executive director of marketing, MeiLin Wan is executive director of textiles and product development, Anna Stec is manager of textiles and project development, and James Hayward is president and CEO of Applied DNA Sciences.